IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

TAASERA LICENSING LLC,	§	Case No. 6:22-cv-01094
Plaintiff,	§	**JURY TRIAL DEMANDED**
v.	§	
CROWDSTRIKE, INC. and CROWDSTRIKE HOLDINGS, INC.,	§	
Defendants.	§	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Taasera Licensing LLC ("Taasera Licensing" or "Plaintiff") for its Complaint against Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc. (collectively, "CrowdStrike" or "Defendants") alleges as follows:

THE PARTIES

1. Taasera Licensing is a limited liability company, organized and existing under the laws of the State of Texas, with its principal place of business located in Plano, Texas.

2. Upon information and belief, CrowdStrike Holdings, Inc. is a publicly traded Delaware corporation with its headquarters and principal place of business in this District at 206 East 9th Street, Suite 1400, Austin, Texas 78701.[1,2] Upon information and belief, CrowdStrike does business in Texas and in the Western District of Texas, directly or through intermediaries, such as

[1] CrowdStrike Holdings, Inc. *Form 10-K 2021, 2022.* Web. 14 April 2022.

[2] https://www.crowdstrike.com/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/

its subsidiaries. Defendant CrowdStrike Holdings, Inc. is the parent of and directly and wholly owns Defendant CrowdStrike, Inc.

3. On information and belief, Defendant CrowdStrike, Inc. is a Delaware corporation, with its headquarters and principal place of business in this District.[3] Defendant CrowdStrike, Inc. is registered with the Secretary of State to conduct business in Texas.

JURISDICTION

4. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has personal jurisdiction over Defendants. Defendants regularly conduct business and have committed acts of patent infringement and/or have induced and are currently inducing acts of patent infringement by others in this Judicial District and/or have contributed and are contributing to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States. Upon information and belief, CrowdStrike conducts business at its headquarters located at 206 East 9th Street, Suite 1400, Austin, Texas 78701.

6. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b) and (c) and 28 U.S.C. § 1400(b) because the Defendants have regular and systematic contacts within this District and have committed acts of infringement in this District. The Defendants, through their own acts, make, use, sell, and/or offer to sell infringing products within this Judicial District, regularly do and solicit business in this Judicial District, and have the requisite minimum contacts within the Judicial District such that this venue is a fair and reasonable one. Upon information and

[3] https://www.crowdstrike.com/blog/crowdstrike-changes-principal-executive-office-to-austin-texas/; https://www.intelligence360.news/crowdstrike-to-spend-447000-00-to-occupy-6385-square-feet-of-space-in-san-antonio-texas/

belief, CrowdStrike directly or indirectly participated in the stream of commerce that results in products, including the Accused Products, being made, used, offered for sale, and/or sold in the State of Texas and/or imported into the United States to the State of Texas.

7. For example, Defendant CrowdStrike Holdings, Inc. leases offices in Texas.[4] Defendant CrowdStrike Holdings, Inc. wholly-owns Defendant CrowdStrike, Inc. and controls Defendant CrowdStrike, Inc., including its contacts with and acts of infringement in this District.[5]

8. On information and belief, Defendant CrowdStrike, Inc. has hundreds of employees in this District—including positions in engineering, sales, marketing, and finance.

9. On information and belief, CrowdStrike's employees located in this District may have relevant information including, in particular, information concerning the products and services Defendants provide and how those products operate.

10. CrowdStrike's operations in this District include client outreach and sales for each of the Accused Products. As detailed above, CrowdStrike has customer-facing personnel and operations in this District. CrowdStrike also provides technical support to partners and customers for its products in this District.

11. On information and belief, CrowdStrike sells, offers for sale, advertises, makes, installs, and/or otherwise provides endpoint security software and security services, including the Accused Products, the use of which infringes the Asserted Patents in this District and the State of

[4] https://ir.crowdstrike.com/sec-filings/sec-filing/10-k/0001535527-21-000007, CrowdStrike U.S. Securities and Exchange Commission Form 10-K for Fiscal Year Ended January 31, 2021 at 52, 125.

[5] https://ir.crowdstrike.com/sec-filings/sec-filing/10-k/0001535527-21-000007, CrowdStrike U.S. Securities and Exchange Commission Form 10-K for Fiscal Year Ended January 31, 2021 at 80, 146; https://www.crowdstrike.com/terms-conditions/.

Texas. CrowdStrike performs these acts directly and/or through its partnerships with other entities.[6]

12. Defendants are subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District, including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

PATENTS-IN-SUIT

13. On March 2, 2010, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,673,137 (the "'137 Patent") entitled "System and Method for the Managed Security Control of Processes on a Computer System." A true and correct copy of the '137 Patent is attached hereto as Exhibit A.

14. On December 4, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,327,441 (the "'441 Patent") entitled "System and Method for Application Attestation." A true and correct copy of the '441 Patent is attached hereto as Exhibit B.

15. On September 30, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,850,517 (the "'517 Patent") entitled "Runtime Risk Detection Based on User, Application, and System Action Sequence Correlation." A true and correct copy of the '517 Patent is attached hereto as Exhibit C.

16. On February 10, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,955,038 (the "'038 Patent") entitled "Methods and Systems for

[6] https://www.crowdstrike.com/partners/solution-providers/

Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '038 Patent is attached hereto as Exhibit D.

17. On March 24, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,990,948 (the "'948 Patent") entitled "Systems and Methods for Orchestrating Runtime Operational Integrity." A true and correct copy of the '948 Patent is attached hereto as Exhibit E.

18. On July 28, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,092,616 (the "'616 Patent") entitled "Systems and Methods for Threat Identification and Remediation." A true and correct copy of the '616 Patent is attached hereto as Exhibit F.

19. On March 28, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,608,997 (the "'997 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '997 Patent is attached hereto as Exhibit G.

20. On March 20, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,923,918 (the "'918 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '918 Patent is attached hereto as Exhibit H.

21. Taasera Licensing is the sole and exclusive owner of all right, title, and interest in the '137 Patent, the '441 Patent, the '517 Patent, the '038 Patent, the '948 Patent, the '616 Patent, the '997 Patent, and the '918 Patent (collectively, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Taasera Licensing also has the right to recover all damages for

past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

FACTUAL ALLEGATIONS

22. The Patents-in-Suit generally cover systems and methods for network security systems.

23. Four of the Patents-in-Suit were invented by International Business Machines ("IBM"). IBM pioneered the field of network security. Every year, IBM spends billions of dollars on research and development to invent, market, and sell new technology, and IBM obtains patents on many of the novel inventions that come out of that work, including the Patents-in-Suit. The six patents invented by IBM are the result of the work from 4 different researchers, spanning over a decade.

24. Four of the Patents-in-Suit were developed by TaaSera, Inc. TaaSera, Inc. was a leader in preemptive breach detection systems, and comprised of security architects and subject matter experts with decades of experience in firewalls, intrusion detection, security event management, malware analysis, and endpoint security. The TaaSera, Inc. patents identify patterns of malicious coordinated network and endpoint behaviors.

25. The '137 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the '137 Patent was developed by Thomas James Satterlee and William Frank Hackenberger of IBM.

26. The '441 Patent generally relates to technology for application attestation. The technology described in the '441 Patent was developed by Srinivas Kumar and Gurudatt Shashikumar of TaaSera, Inc.

27. The ’517 Patent generally relates to runtime risk detection based on user, application, and/or system actions. The technology described in the ’517 Patent was developed by Srinivas Kumar of TaaSera, Inc.

28. The ’038 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the ’038 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

29. The ’948 Patent generally relates to technology that provides runtime operational integrity profiles identifying a threat level of subjects or applications. The technology described in the ’948 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

30. The ’616 Patent generally relates to technology that provides integrity profiles identifying a threat level of a system. The technology described in the ’616 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

31. The ’997 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the ’997 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

32. The ’918 Patent generally relates to technology that controls access to computing resources based on known security vulnerabilities. The technology described in the ’918 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

33. Defendants have infringed and continue to infringe one or more of the Patents-in-Suit by making, using, selling, offering to sell, and/or importing, and by actively inducing others to make, use, sell, offer to sell, and/or import products that implement the network security inventions claimed in the Patents-in-Suit. For example, the Accused Products include at least

CrowdStrike Falcon Insight EDR (with Falcon Agent), CrowdStrike Falcon Insight EDR (with Falcon Agent) and with Falcon Agentand Falcon Spotlight.

34. TaaSera, Inc. manufactured commercial and academic versions of its NetTrust Security Appliance. NetTrust combined breach detection with security analytics to identify hidden threatening network behaviors. The analytics engine analyzed behavioral profiles, threat patterns, and contextual evidence to rank systems by their risk of breach.

35. Upon information and belief, Taasera Licensing and its predecessors have complied with the requirements of 35 U.S.C. § 287(a).

COUNT I
(Infringement of the ’137 Patent)

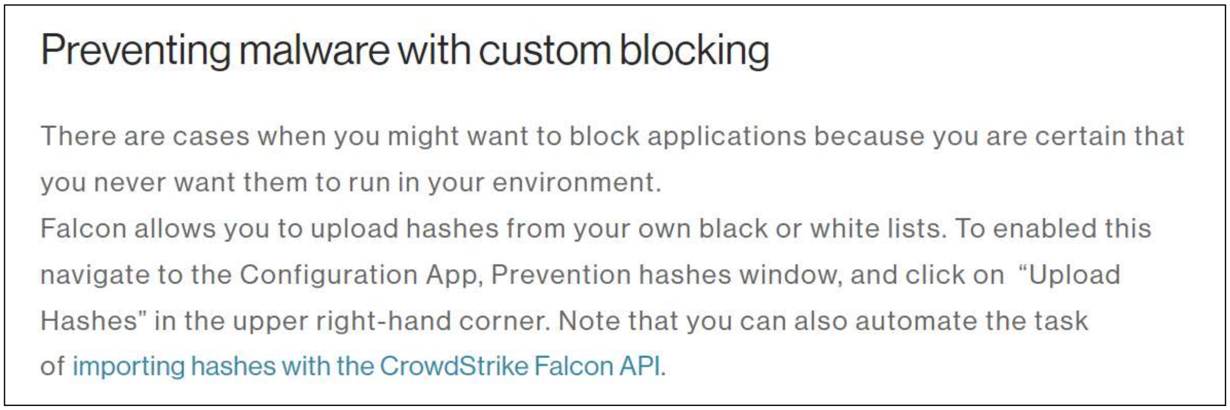
36. Paragraphs 1 through 35 are incorporated by reference as if fully set forth herein.

37. Defendants are not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’137 Patent.

38. Defendants have and continue to directly infringe at least claim 6 of the ’137 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’137 Patent. Such products incorporate the Custom Application Blocking and Kernel Exploit Prevention features and include at least CrowdStrike Falcon Insight EDR (with Falcon Agent) (the “’137 Accused Product”) which practice a method for implementing security for a computing device comprising the steps of: interrupting the loading of a new program for operation with the computing device; validating the new program; if the new program is validated, permitting the new program to continue loading and to execute in connection with the computing device; if the new program is not validated, monitoring the new program while it loads and executes in connection with the

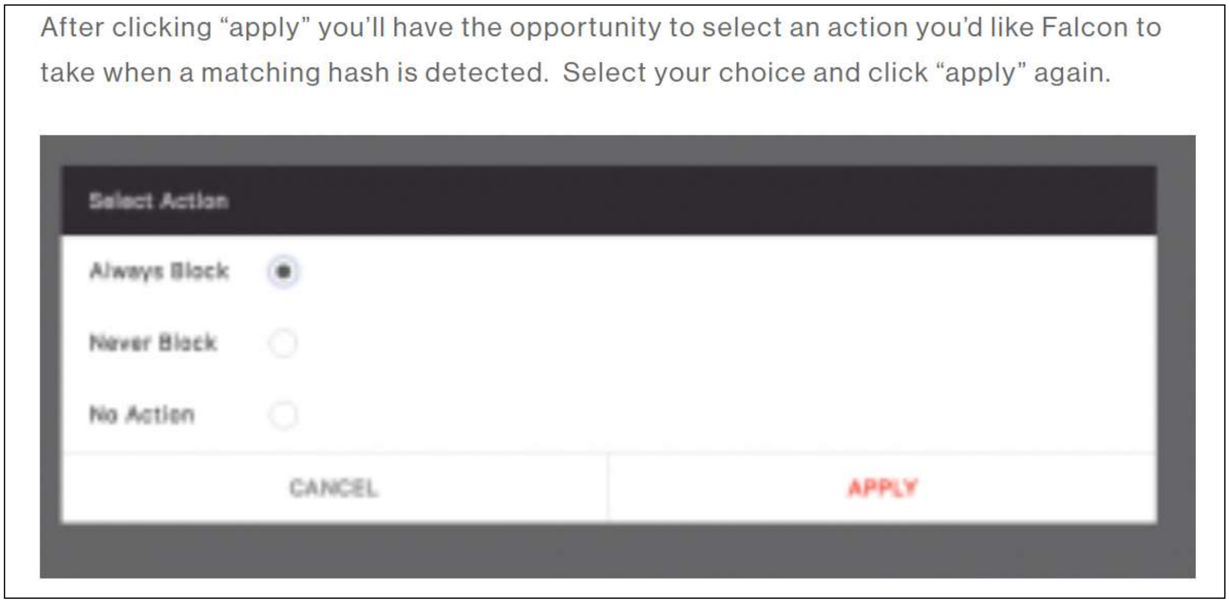
computing device, wherein the step of monitoring the new program while it executes is performed at the operating system kernel of the computing device.

39. Every ’137 Accused Product practices interrupting the loading of a new program for operation with the computing device. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) performs custom application blocking.



Preventing malware with custom blocking

There are cases when you might want to block applications because you are certain that you never want them to run in your environment.
Falcon allows you to upload hashes from your own black or white lists. To enabled this navigate to the Configuration App, Prevention hashes window, and click on "Upload Hashes" in the upper right-hand corner. Note that you can also automate the task of importing hashes with the CrowdStrike Falcon API.



After clicking "apply" you'll have the opportunity to select an action you'd like Falcon to take when a matching hash is detected. Select your choice and click "apply" again.

Select Action

Always Block ●

Never Block ○

No Action ○

[7]

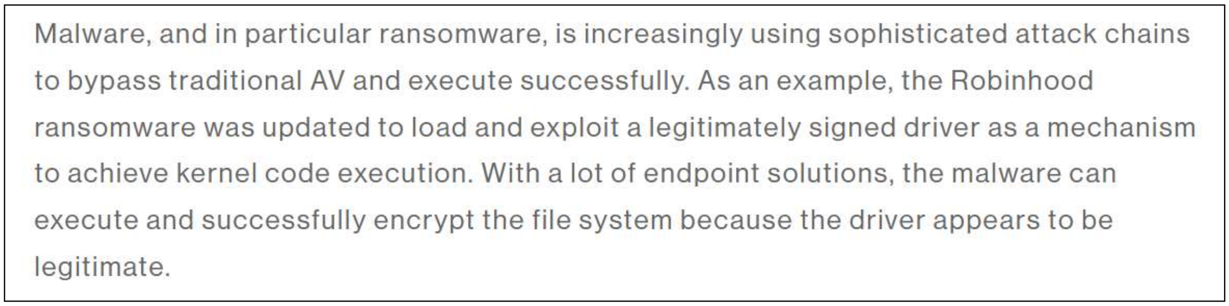
40. Every ’137 Accused Product practices permitting the new program to continue loading and executing in connection with the computing device if the new program is validated.

[7] https://www.crowdstrike.com/blog/tech-center/how-to-prevent-malware-with-custom-blacklisting/

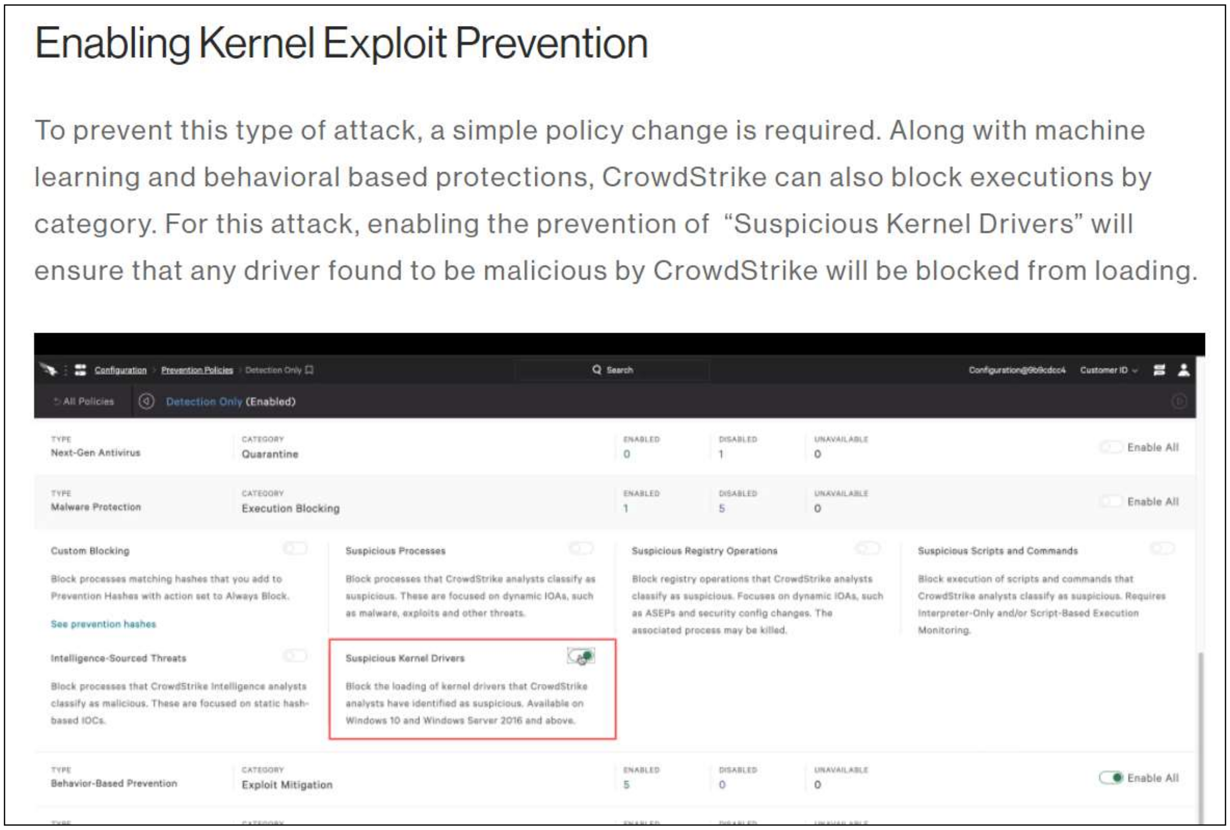
For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) permits new programs to run if the new program was not blocked by the Custom Application Blocking feature.[8]

41. Every ’137 Accused Product practices monitoring the new program while it loads and executes in connection with the computer device. For example, if the new program passes CrowdStrike Falcon Insight EDR (with Falcon Agent) Custom Application Blocking feature, it will continue to be monitored by CrowdStrike Kernel Exploit Prevention, for example, to determine if it exhibits suspicious behavior.

[8] *Id.*



Malware, and in particular ransomware, is increasingly using sophisticated attack chains to bypass traditional AV and execute successfully. As an example, the Robinhood ransomware was updated to load and exploit a legitimately signed driver as a mechanism to achieve kernel code execution. With a lot of endpoint solutions, the malware can execute and successfully encrypt the file system because the driver appears to be legitimate.



Enabling Kernel Exploit Prevention

To prevent this type of attack, a simple policy change is required. Along with machine learning and behavioral based protections, CrowdStrike can also block executions by category. For this attack, enabling the prevention of "Suspicious Kernel Drivers" will ensure that any driver found to be malicious by CrowdStrike will be blocked from loading.

Detection Only (Enabled)

TYPE	CATEGORY	ENABLED	DISABLED	UNAVAILABLE	
Next-Gen Antivirus	Quarantine	0	1	0	Enable All
Malware Protection	Execution Blocking	1	5	0	Enable All

Custom Blocking

Block processes matching hashes that you add to Prevention Hashes with action set to Always Block.

See prevention hashes

Suspicious Processes

Block processes that CrowdStrike analysts classify as suspicious. These are focused on dynamic IOAs, such as malware, exploits and other threats.

Suspicious Registry Operations

Block registry operations that CrowdStrike analysts classify as suspicious. Focuses on dynamic IOAs, such as ASEPs and security config changes. The associated process may be killed.

Suspicious Scripts and Commands

Block execution of scripts and commands that CrowdStrike analysts classify as suspicious. Requires Interpreter-Only and/or Script-Based Execution Monitoring.

Intelligence-Sourced Threats

Block processes that CrowdStrike Intelligence analysts classify as malicious. These are focused on static hash-based IOCs.

Suspicious Kernel Drivers

Block the loading of kernel drivers that CrowdStrike analysts have identified as suspicious. Available on Windows 10 and Windows Server 2016 and above.

TYPE	CATEGORY	ENABLED	DISABLED	UNAVAILABLE	
Behavior-Based Prevention	Exploit Mitigation	5	0	0	Enable All

[9]

42. Defendants have and continue to indirectly infringe one or more claims of the '137 Patent by knowingly and intentionally inducing others, including CrowdStrike subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as the '137 Accused Product (*e.g.*, products incorporating the Custom Application Blocking and Kernel Exploit Prevention features).

[9] https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/

43. Defendants with knowledge that these products, or the use thereof, infringe the '137 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continue to knowingly and intentionally induce, direct infringement of the '137 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on their support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[10]

44. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing and maintaining those products, and provides technical support to users via the CrowdStrike support portal.[11]

45. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the "CrowdStrike Falcon agent" to be installed on individual endpoint computers.[12]

46. Defendants have induced and are currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '137 Patent, but while remaining willfully blind to the infringement.

47. Taasera Licensing has suffered damages as a result of Defendants' direct and indirect infringement of the '137 Patent in an amount to be proved at trial.

[10] https://www.crowdstrike.com/products/crowdstrike-support/

[11] *Id.*

[12] https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/

48. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendants' infringement of the '137 Patent, for which there is no adequate remedy at law, unless Defendants' infringement is enjoined by this Court.

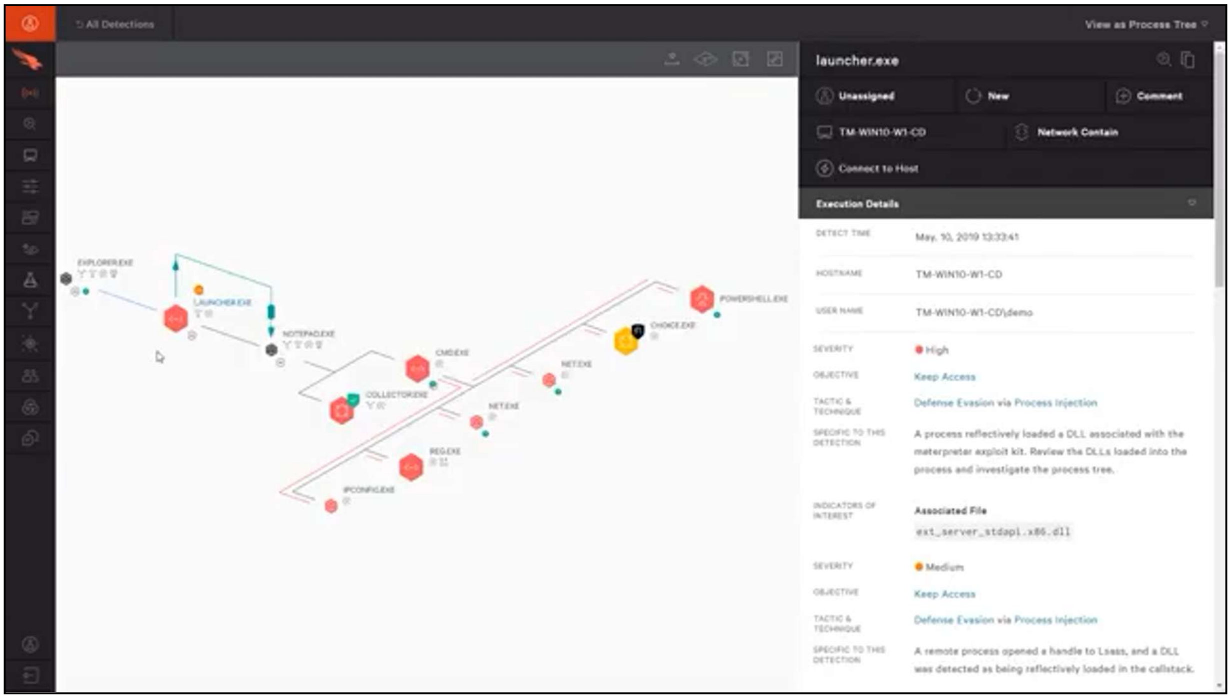
COUNT II
(Infringement of the '441 Patent)

49. Paragraphs 1 through 35 are incorporated by reference as if fully set forth herein.

50. Defendants are not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '441 Patent.

51. Defendants have and continue to directly infringe at least claim 1 of the '441 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '441 Patent. Such products incorporate the endpoint detection feature and include at least CrowdStrike Falcon Insight EDR (with Falcon Agent) (the "'441 Accused Product") which practice a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server, comprising: receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components; generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application.

52. Every ’441 Accused Product practices a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) analyzes endpoint activity to automatically identify attacker behavior.



launcher.exe

TM-WIN10-W1-CD

DETECT TIME: May. 10, 2019 13:33:41

HOSTNAME: TM-WIN10-W1-CD

USER NAME: TM-WIN10-W1-CD\demo

SEVERITY: High

OBJECTIVE: Keep Access

TACTIC & TECHNIQUE: Defense Evasion via Process Injection

SPECIFIC TO THIS DETECTION: A process reflectively loaded a DLL associated with the meterpreter exploit kit. Review the DLLs loaded into the process and investigate the process tree.

INDICATORS OF INTEREST: Associated File `ext_server_stdapi.x86.dll`

SEVERITY: Medium

OBJECTIVE: Keep Access

TACTIC & TECHNIQUE: Defense Evasion via Process Injection

SPECIFIC TO THIS DETECTION: A remote process opened a handle to Lsass, and a DLL was detected as being reflectively loaded in the callstack.

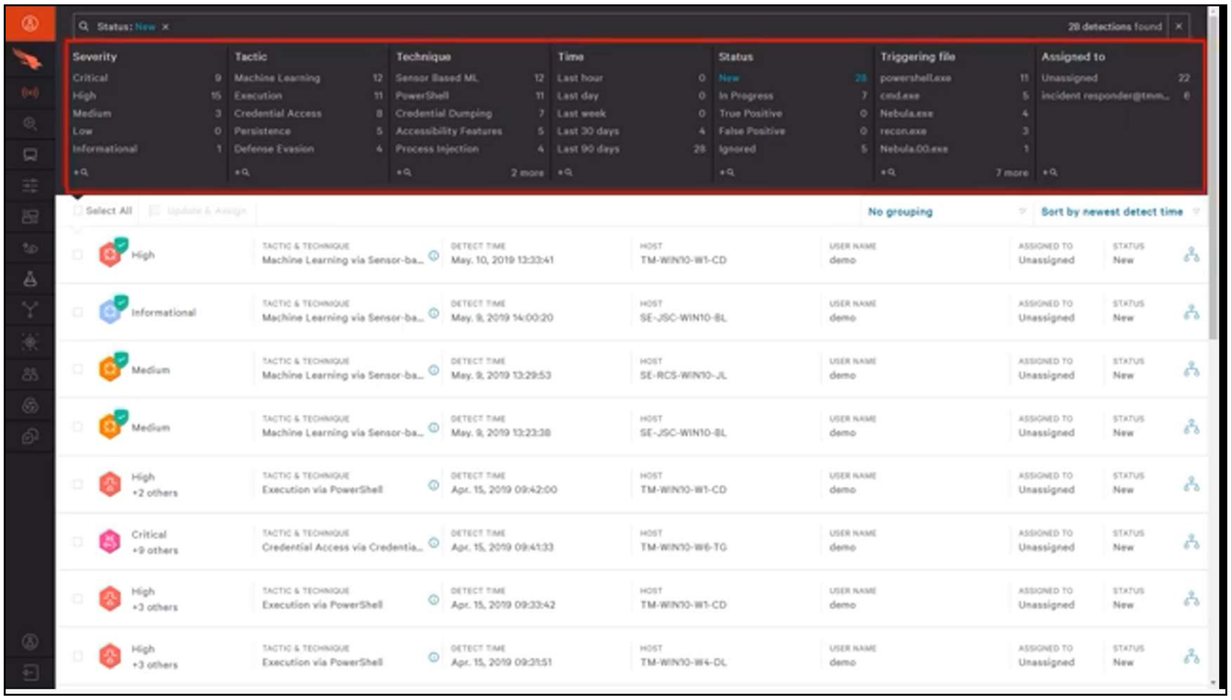
[13]

53. Every ’441 Accused Product practices receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application, and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components. For example, CrowdStrike Falcon

[13] https://www.crowdstrike.com/resources/videos/video-demonstration-of-falcon-endpoint-protection-enterprise/

Insight EDR (with Falcon Agent) receives process attributes, context information, and processes behavior information for detected threats.[14]

54. Every ’441 Accused Product practices generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) generates alerts and reports prioritized detected threats.



Status: New ×

28 detections found ×

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	9	Machine Learning	12	Sensor Based ML	12	Last hour	0	New	28	powershell.exe	11	Unassigned	22
High	15	Execution	11	PowerShell	11	Last day	0	In Progress	7	cmd.exe	5	incident responder@tmm...	6
Medium	3	Credential Access	8	Credential Dumping	7	Last week	0	True Positive	0	Nebula.exe	4		
Low	0	Persistence	5	Accessibility Features	5	Last 30 days	4	False Positive	0	recon.exe	3		
Informational	1	Defense Evasion	4	Process Injection	4	Last 90 days	28	Ignored	5	Nebula.00.exe	1		
					2 more						7 more		

□ Select All Update & Assign

No grouping

Sort by newest detect time

	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High	Machine Learning via Sensor-ba...	May. 10, 2019 13:33:41	TM-WIN10-W1-CD	demo	Unassigned	New
Informational	Machine Learning via Sensor-ba...	May. 9, 2019 14:00:20	SE-JSC-WIN10-BL	demo	Unassigned	New
Medium	Machine Learning via Sensor-ba...	May. 9, 2019 13:29:53	SE-RCS-WIN10-JL	demo	Unassigned	New
Medium	Machine Learning via Sensor-ba...	May. 9, 2019 13:23:38	SE-JSC-WIN10-BL	demo	Unassigned	New
High +2 others	Execution via PowerShell	Apr. 15, 2019 09:42:00	TM-WIN10-W1-CD	demo	Unassigned	New
Critical +9 others	Credential Access via Credentia...	Apr. 15, 2019 09:41:33	TM-WIN10-W6-TG	demo	Unassigned	New
High +3 others	Execution via PowerShell	Apr. 15, 2019 09:33:42	TM-WIN10-W1-CD	demo	Unassigned	New
High +3 others	Execution via PowerShell	Apr. 15, 2019 09:31:51	TM-WIN10-W4-DL	demo	Unassigned	New

15

55. Defendants have and continue to indirectly infringe one or more claims of the ’441 Patent by knowingly and intentionally inducing others, including CrowdStrike subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that

[14] *Id.*

[15] https://www.youtube.com/watch?v=VuiPG1PiMsM

include infringing technology, such as the ’441 Accused Product (*e.g.*, products incorporating the predictive machine learning feature).

56. Defendants with knowledge that these products, or the use thereof, infringe the ’441 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’441 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on their support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[16]

57. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing and maintaining those products, and provides technical support to users via the CrowdStrike support portal.[17]

58. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the “CrowdStrike Falcon agent” to be installed on individual endpoint computers.[18]

59. Defendants have induced and are currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’441 Patent, but while remaining willfully blind to the infringement.

[16] https://www.crowdstrike.com/products/crowdstrike-support/

[17] *Id.*

[18] https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/

60. Taasera Licensing has suffered damages as a result of Defendants' direct and indirect infringement of the '441 Patent in an amount to be proved at trial.

61. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendants' infringement of the '441 Patent, for which there is no adequate remedy at law, unless Defendants' infringement is enjoined by this Court.

COUNT III
(Infringement of the '038 Patent)

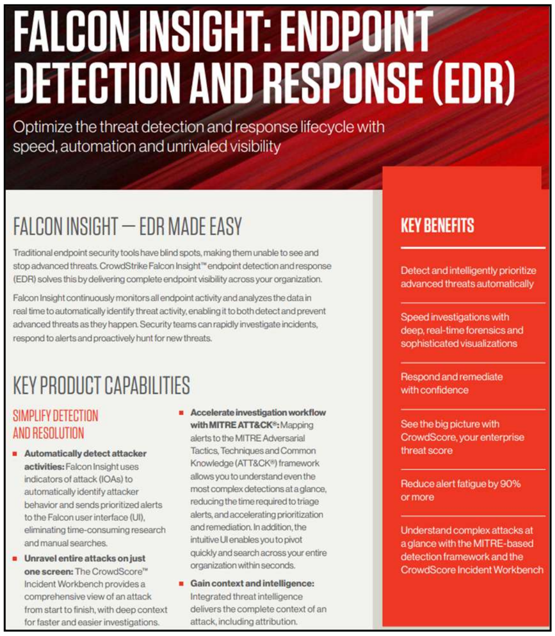
62. Paragraphs 1 through 35 are incorporated by reference as if fully set forth herein.

63. Defendants are not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '038 Patent.

64. Defendants have and continue to directly infringe at least claim 1 of the '038 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '038 Patent. Such products include at least CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight (the "'038 Accused Products") which is a system for controlling the operation of an endpoint and comprises a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to: receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents, determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and initiate, based on the

compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint.

65. Every ’038 Accused Product controls the operation of an endpoint. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight controls the operation of an endpoint.



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

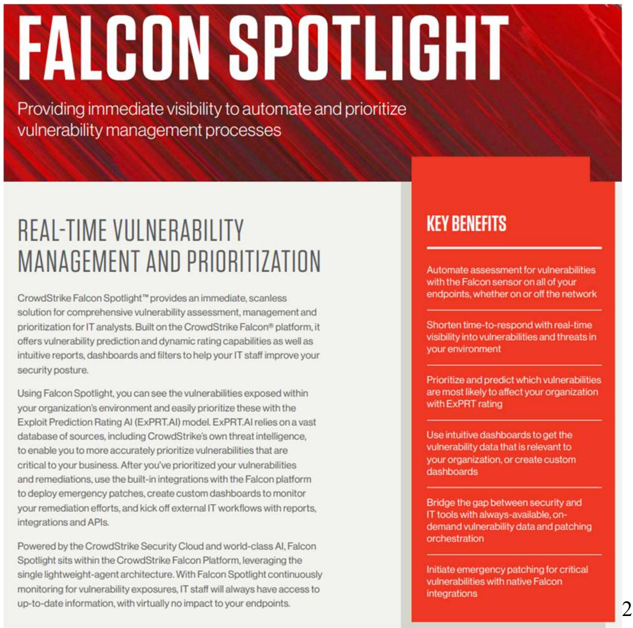
Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[19]



FALCON SPOTLIGHT

Providing immediate visibility to automate and prioritize vulnerability management processes

REAL-TIME VULNERABILITY MANAGEMENT AND PRIORITIZATION

CrowdStrike Falcon Spotlight™ provides an immediate, scanless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. Built on the CrowdStrike Falcon® platform, it offers vulnerability prediction and dynamic rating capabilities as well as intuitive reports, dashboards and filters to help your IT staff improve your security posture.

Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.

Powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight sits within the CrowdStrike Falcon Platform, leveraging the single lightweight-agent architecture. With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.

KEY BENEFITS

Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network

Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment

Prioritize and predict which vulnerabilities are most likely to affect your organization with ExPRT rating

Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards

Bridge the gap between security and IT tools with always-available, on-demand vulnerability data and patching orchestration

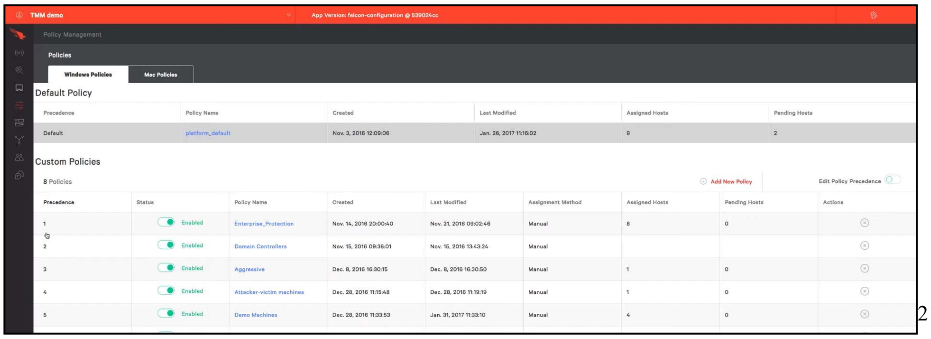
Initiate emergency patching for critical vulnerabilities with native Falcon integrations

[20]

66. Every ’038 Accused Product comprises a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies, and a data store, at the computing system, that contains the plurality of policies. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) allows configuration of a plurality of policies at a system remote from the endpoint through a provided user interface which are stored in a data store.

[19] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

[20] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-spotlight-data-sheet.pdf



TMM demo

App Version: falcon-configuration @ 539024cc

Policy Management

Policies

Windows Policies | Mac Policies

Default Policy

Precedence	Policy Name	Created	Last Modified	Assigned Hosts	Pending Hosts
Default	platform_default	Nov. 3, 2016 12:09:06	Jan. 26, 2017 11:16:02	9	2

Custom Policies

8 Policies

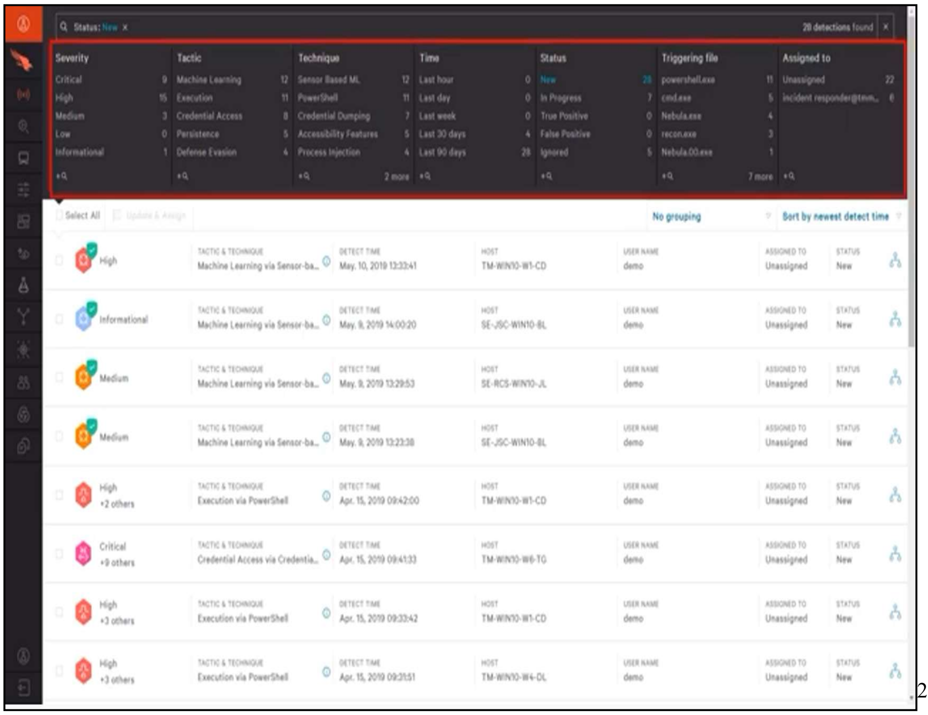
Add New Policy

Edit Policy Precedence

Precedence	Status	Policy Name	Created	Last Modified	Assignment Method	Assigned Hosts	Pending Hosts	Actions
1	Enabled	Enterprise_Protection	Nov. 14, 2016 20:00:40	Nov. 21, 2016 09:02:46	Manual	8	0	⊗
2	Enabled	Domain Controllers	Nov. 15, 2016 09:38:01	Nov. 15, 2016 13:43:24	Manual			⊗
3	Enabled	Aggressive	Dec. 8, 2016 16:30:15	Dec. 8, 2016 16:30:50	Manual	1	0	⊗
4	Enabled	Attacker-victim machines	Dec. 28, 2016 11:15:48	Dec. 28, 2016 11:19:19	Manual	1	0	⊗
5	Enabled	Demo Machines	Dec. 28, 2016 11:33:53	Jan. 31, 2017 11:33:10	Manual	4	0	⊗

[21]

67. Every '038 Accused Product comprises one or more software agents on the endpoint configured to monitor the plurality of operating conditions identified in the plurality of policies. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) comprises the Falcon sensor that detects file I/O operations, privilege escalation, and behavioral IOAs identified in the plurality of policies.



Status: New ×

28 detections found

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	9	Machine Learning	12	Sensor Based ML	12	Last hour	0	New	28	powershell.exe	11	Unassigned	22
High	15	Execution	11	PowerShell	11	Last day	0	In Progress	7	cmd.exe	5	incident responder@tmm...	6
Medium	3	Credential Access	8	Credential Dumping	7	Last week	0	True Positive	0	Nebula.exe	4		
Low	0	Persistence	5	Accessibility Features	5	Last 30 days	4	False Positive	0	recon.exe	3		
Informational	1	Defense Evasion	4	Process Injection	4	Last 90 days	28	Ignored	5	Nebula.00.exe	1		
					2 more						7 more		

Select All | Update & Assign

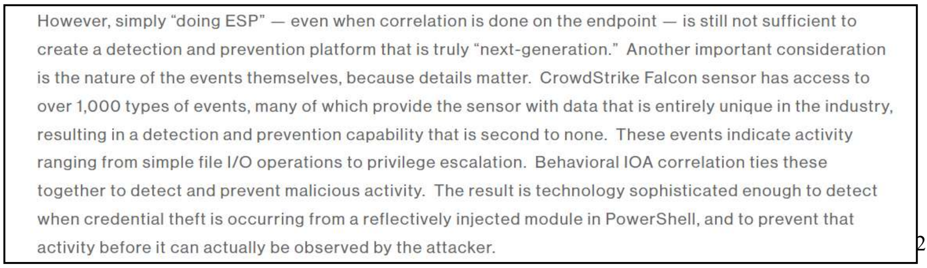
No grouping

Sort by newest detect time

	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High	Machine Learning via Sensor-ba...	May. 10, 2019 13:33:41	TM-WIN10-W1-CD	demo	Unassigned	New
Informational	Machine Learning via Sensor-ba...	May. 9, 2019 14:00:20	SE-JSC-WIN10-BL	demo	Unassigned	New
Medium	Machine Learning via Sensor-ba...	May. 9, 2019 13:29:53	SE-RCS-WIN10-JL	demo	Unassigned	New
Medium	Machine Learning via Sensor-ba...	May. 9, 2019 13:23:38	SE-JSC-WIN10-BL	demo	Unassigned	New
High +2 others	Execution via PowerShell	Apr. 15, 2019 09:42:00	TM-WIN10-W1-CD	demo	Unassigned	New
Critical +9 others	Credential Access via Credentia...	Apr. 15, 2019 09:41:33	TM-WIN10-W6-TG	demo	Unassigned	New
High +3 others	Execution via PowerShell	Apr. 15, 2019 09:33:42	TM-WIN10-W1-CD	demo	Unassigned	New
High +3 others	Execution via PowerShell	Apr. 15, 2019 09:31:51	TM-WIN10-W4-DL	demo	Unassigned	New

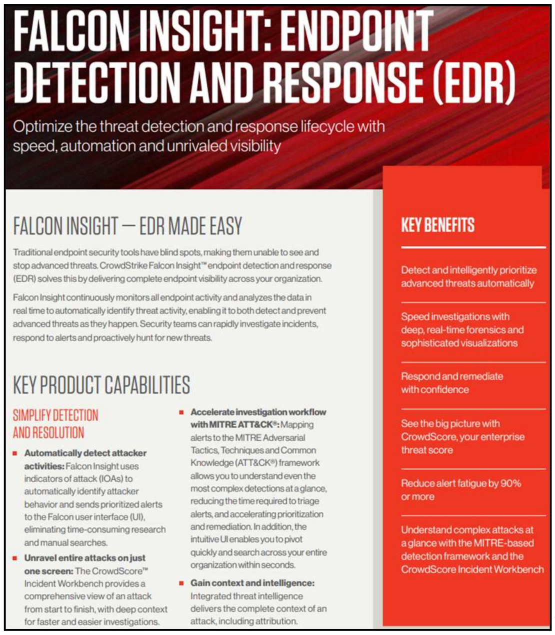
[22]

[21] https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/
[22] https://www.youtube.com/watch?v=VuiPG1PiMsM



However, simply "doing ESP" — even when correlation is done on the endpoint — is still not sufficient to create a detection and prevention platform that is truly "next-generation." Another important consideration is the nature of the events themselves, because details matter. CrowdStrike Falcon sensor has access to over 1,000 types of events, many of which provide the sensor with data that is entirely unique in the industry, resulting in a detection and prevention capability that is second to none. These events indicate activity ranging from simple file I/O operations to privilege escalation. Behavioral IOA correlation ties these together to detect and prevent malicious activity. The result is technology sophisticated enough to detect when credential theft is occurring from a reflectively injected module in PowerShell, and to prevent that activity before it can actually be observed by the attacker.[23]

68. Every '038 Accused Product practices receiving, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) detects and receives alerts for suspicious endpoint activity gathered by the Falcon sensor.[24]



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[25]

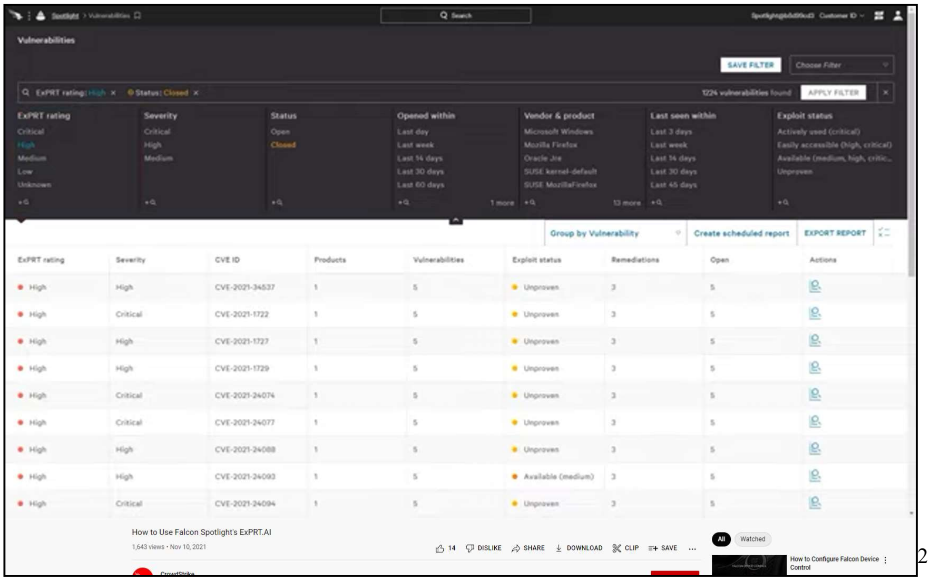
69. Every '038 Accused Product practices determining a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight

[23] https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/

[24] https://www.youtube.com/watch?v=VuiPG1PiMsM

[25] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

determines a compliance state of the endpoint based on the exploit status and a plurality of compliance policies.



ExPRT rating	Severity	CVE ID	Products	Vulnerabilities	Exploit status	Remediations	Open	Actions
● High	High	CVE-2021-34537	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-1722	1	5	● Unproven	3	5	
● High	High	CVE-2021-1727	1	5	● Unproven	3	5	
● High	High	CVE-2021-1729	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-24074	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-24077	1	5	● Unproven	3	5	
● High	High	CVE-2021-24088	1	5	● Unproven	3	5	
● High	High	CVE-2021-24093	1	5	● Available (medium)	3	5	
● High	Critical	CVE-2021-24094	1	5	● Unproven	3	5	

How to Use Falcon Spotlight's ExPRT.AI

1,643 views • Nov 10, 2021

[26]

70. Every ’038 Accused Product practices initiating, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight provides an “Install Patch” button when a patch is required. The patch is installed by the endpoint.[27]

> After selecting a specific host or recommended patch will provide additional details and access to the “Install Patch” button. Clicking the ‘Install Patch’, the host’s local Windows Update service will attempt to download and install the patch. A success message indicates that the process has started, not that it has completed; depending on the size of the patch, this could take some time.

[28]

71. Defendants have and continue to indirectly infringe one or more claims of the ’038 Patent by knowingly and intentionally inducing others, including CrowdStrike subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents,

[26] https://www.youtube.com/watch?v=P1qOGCeEYK8
[27] *Id.*
[28] https://www.crowdstrike.com/blog/tech-center/emergency-patching/

by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’038 Accused Products (*e.g.*, products incorporating the Vulnerability Management feature).

72. Defendants with knowledge that these products, or the use thereof, infringe the ’038 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’038 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on their support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[29]

73. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing and maintaining those products, and provides technical support to users via the CrowdStrike support portal.[30]

74. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the “CrowdStrike Falcon agent” to be installed on individual endpoint computers.[31]

75. Defendants have induced and are currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’038 Patent, but while remaining willfully blind to the infringement.

[29] https://www.crowdstrike.com/products/crowdstrike-support/

[30] *Id.*

[31] https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/

76. Taasera Licensing has suffered damages as a result of Defendants' direct and indirect infringement of the '038 Patent in an amount to be proved at trial.

77. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendants' infringement of the '038 Patent, for which there is no adequate remedy at law, unless Defendants' infringement is enjoined by this Court.

COUNT IV
(Infringement of the '948 Patent)

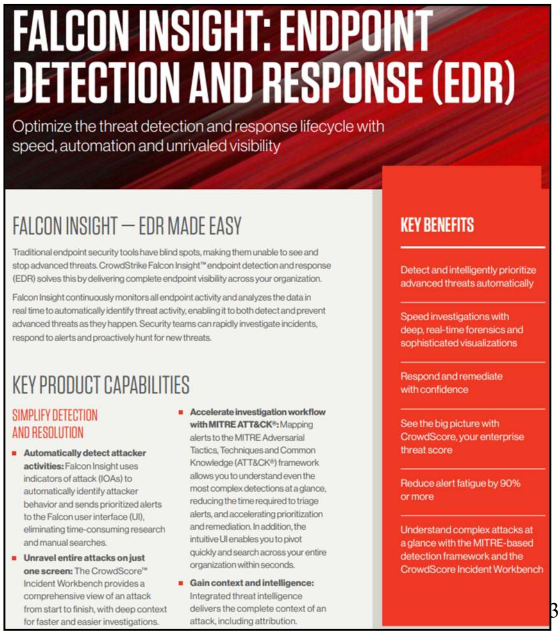
78. Paragraphs 1 through 35 are incorporated by reference as if fully set forth herein.

79. Defendants are not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '948 Patent.

80. Defendants have and continue to directly infringe at least claim 1 of the '948 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '948 Patent. Such products incorporate the Extended Detection and Response feature and include at least CrowdStrike Falcon Insight EDR (with Falcon Agent) (the "'948 Accused Product") which practices a method of providing real-time operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat

classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.

81. Every ’948 Accused Product practices a method of providing real-time operational integrity of an application on a native computing environment. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) incorporates application integrity monitoring and behavior analysis.



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

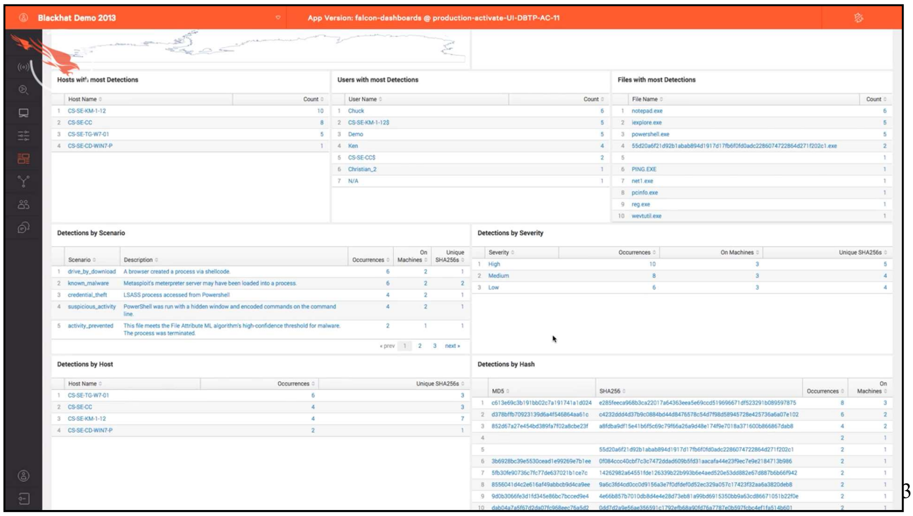
See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[32]

[32] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf



Blackhat Demo 2013
App Version: falcon-dashboards @ production-activate-UI-DBTP-AC-11

Hosts with most Detections

	Host Name	Count
1	CS-SE-KM-1-12	10
2	CS-SE-CC	8
3	CS-SE-TG-W7-01	5
4	CS-SE-CD-WIN7-P	1

Users with most Detections

	User Name	Count
1	Chuck	6
2	CS-SE-KM-1-12$	5
3	Demo	5
4	Ken	4
5	CS-SE-CC$	2
6	Christian_2	1
7	N/A	1

Files with most Detections

	File Name	Count
1	notepad.exe	6
2	iexplore.exe	5
3	powershell.exe	5
4	55d20a6f21d92b1abab894d1917d17fb6f0fd0adc2286074722864d271f202c1.exe	2
5		1
6	PING.EXE	1
7	net1.exe	1
8	pcinfo.exe	1
9	reg.exe	1
10	wevtutil.exe	1

Detections by Scenario

	Scenario	Description	Occurrences	On Machines	Unique SHA256s
1	drive_by_download	A browser created a process via shellcode.	6	2	1
2	known_malware	Metasploit's meterpreter server may have been loaded into a process.	6	2	2
3	credential_theft	LSASS process accessed from Powershell	4	2	1
4	suspicious_activity	PowerShell was run with a hidden window and encoded commands on the command line.	4	2	1
5	activity_prevented	This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was terminated.	2	1	1

« prev 1 2 3 next »

Detections by Severity

	Severity	Occurrences	On Machines	Unique SHA256s
1	High	10	3	5
2	Medium	8	3	4
3	Low	6	3	4

Detections by Host

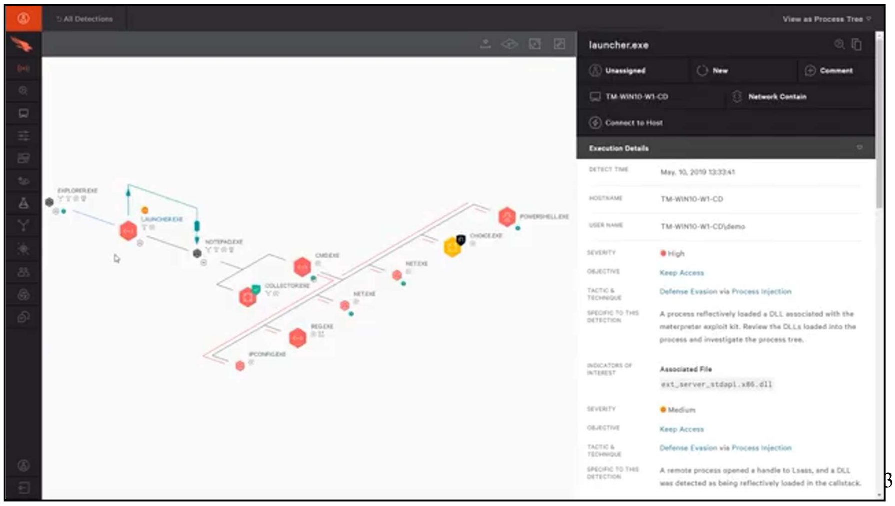
	Host Name	Occurrences	Unique SHA256s
1	CS-SE-TG-W7-01	6	3
2	CS-SE-CC	4	3
3	CS-SE-KM-1-12	4	7
4	CS-SE-CD-WIN7-P	2	1

Detections by Hash

	MD5	SHA256	Occurrences	On Machines
1	c613e69c3b191bb02c7a191741a1d024	e285feeca968b3ca22017a64363eea5e69ccd519696671df523291b089597875	8	3
2	d378bffb70923139d6a4f546864aa61c	c4232ddd4d37b9c0884bd44d8476578c54d7f98d58945728e425736a6a07e102	6	2
3	852d67a27e454bd389fa7f02a8cbe23f	a8fdba9df15e41b6f5c69c79f66a26a9d48e174f9e7018a371600b866867dab8	4	2
4			2	1
5		55d20a6f21d92b1abab894d1917d17fb6f0fd0adc2286074722864d271f202c1	2	1
6	3b6928bc39e5530cead1e99269e7b1ee	0f084ccc40cbf7c3c7472ddad609b5fd31aacafa44e23f9ec7e9e2184713b986	2	1
7	5fb30fe90736c7fc77de637021b1ce7c	14262982a64551fde126339b22b993b6e4aed520e53dd882e67d887b6b66f942	2	1
8	8556041d4c2e616af49abbcb9d4ca9ee	9a6c3fd4cd0cc0d9156a3e7f0dfdef0d52ec329a057c17423f32aa6a3820deb8	2	1
9	9d0b3066fe3d1fd345e86bc7bcced9e4	4e66b857b7010db8d4e4e28d73eb81a99bd6915350bb9a63cd86671051b22f0e	2	1
10	dab04a7a5f67d2da07fc968eec76a5d2	0dd7d2a9e56ae356591c1792efb68a90fd76a7787e0b597fcbc4ef1fa514b601	2	1

[33]

82. Every '948 Accused Product practices monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) monitors endpoint activity and performs real-time forensics with context and attribution.[34]



launcher.exe

TM-WIN10-W1-CD

Execution Details

DETECT TIME May. 10, 2019 13:33:41

HOSTNAME TM-WIN10-W1-CD

USER NAME TM-WIN10-W1-CD\demo

SEVERITY ● High

OBJECTIVE Keep Access

TACTIC & TECHNIQUE Defense Evasion via Process Injection

SPECIFIC TO THIS DETECTION A process reflectively loaded a DLL associated with the materpreter exploit kit. Review the DLLs loaded into the process and investigate the process tree.

INDICATORS OF INTEREST Associated File `ext_server_stdapi.x86.dll`

SEVERITY ● Medium

OBJECTIVE Keep Access

TACTIC & TECHNIQUE Defense Evasion via Process Injection

SPECIFIC TO THIS DETECTION A remote process opened a handle to Lsass, and a DLL was detected as being reflectively loaded in the callstack.

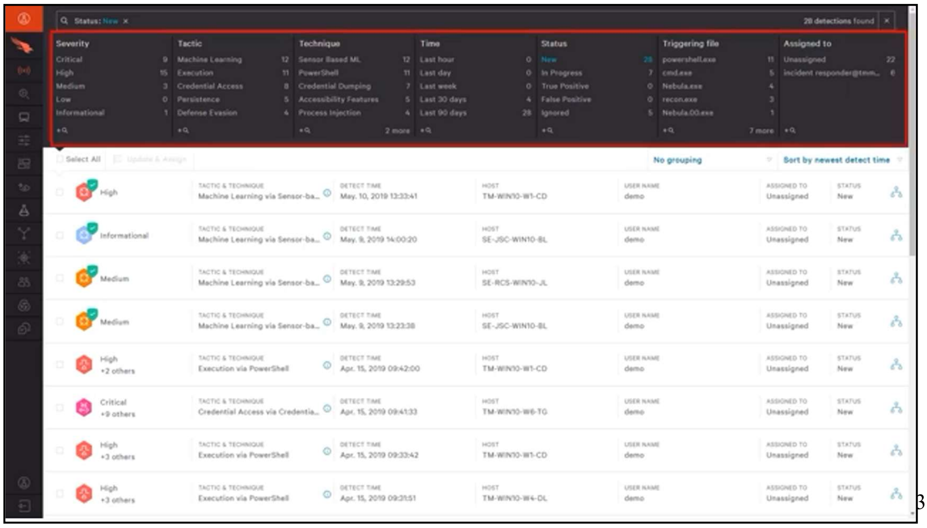
[35]

[33] https://www.youtube.com/watch?v=IJARP_4vcHM

[34] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

[35] https://www.crowdstrike.com/resources/videos/video-demonstration-of-falcon-endpoint-protection-enterprise/

83. Every ’948 Accused Product practices generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) security agents generate behavior based events for determining the real time operational integrity of the application executing on the native computer environment. [36]



Status: New ×

28 detections found ×

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	9	Machine Learning	12	Sensor Based ML	12	Last hour	0	New	28	powershell.exe	11	Unassigned	22
High	15	Execution	11	PowerShell	11	Last day	0	In Progress	7	cmd.exe	5	incident responder@tmm...	6
Medium	3	Credential Access	8	Credential Dumping	7	Last week	0	True Positive	0	Nebula.exe	4		
Low	0	Persistence	5	Accessibility Features	5	Last 30 days	4	False Positive	0	recon.exe	3		
Informational	1	Defense Evasion	4	Process Injection	4	Last 90 days	28	Ignored	5	Nebula.00.exe	1		
					2 more						7 more		

Select All Update & Assign No grouping Sort by newest detect time

	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High	Machine Learning via Sensor-ba...	May. 10, 2019 13:33:41	TM-WIN10-W1-CD	demo	Unassigned	New
Informational	Machine Learning via Sensor-ba...	May. 9, 2019 14:00:20	SE-JSC-WIN10-BL	demo	Unassigned	New
Medium	Machine Learning via Sensor-ba...	May. 9, 2019 13:29:53	SE-RCS-WIN10-JL	demo	Unassigned	New
Medium	Machine Learning via Sensor-ba...	May. 9, 2019 13:23:38	SE-JSC-WIN10-BL	demo	Unassigned	New
High +2 others	Execution via PowerShell	Apr. 15, 2019 09:42:00	TM-WIN10-W1-CD	demo	Unassigned	New
Critical +9 others	Credential Access via Credentia...	Apr. 15, 2019 09:41:33	TM-WIN10-W6-TG	demo	Unassigned	New
High +3 others	Execution via PowerShell	Apr. 15, 2019 09:33:42	TM-WIN10-W1-CD	demo	Unassigned	New
High +3 others	Execution via PowerShell	Apr. 15, 2019 09:31:51	TM-WIN10-W4-DL	demo	Unassigned	New

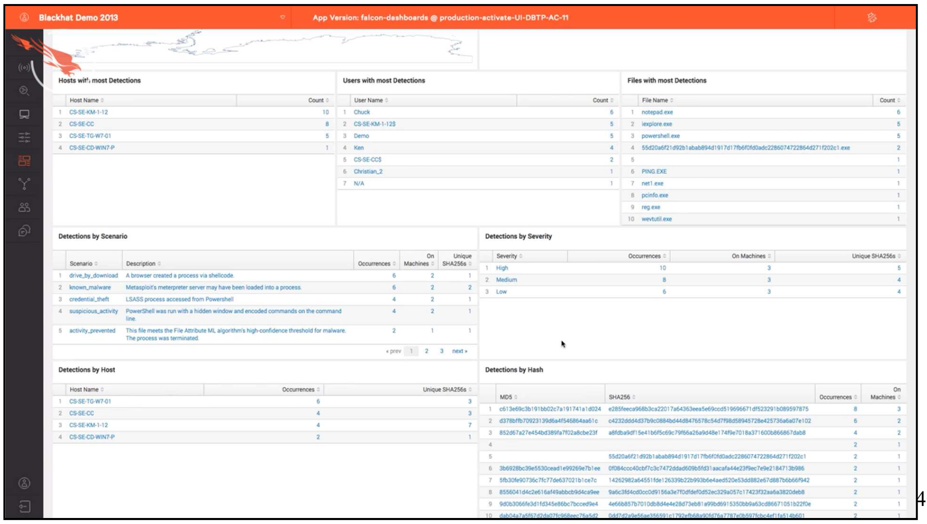
[37]

84. Every ’948 Accused Product practices correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events. For example, the MITRE ATT&CK framework correlates threat classifications based on the temporal sequence of detected behavioral events.[38]

85. Every ’948 Accused Product practices displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status

[36] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf
[37] https://www.youtube.com/watch?v=VuiPG1PiMsM
[38] *Id*.

indications for operational integrity of the application. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) includes several display options for showing real-time status indications for the operational integrity of the application.[39]



Blackhat Demo 2013

App Version: falcon-dashboards @ production-activate-UI-DBTP-AC-11

Hosts with most Detections

	Host Name	Count
1	CS-SE-KM-1-12	10
2	CS-SE-CC	8
3	CS-SE-TG-W7-01	5
4	CS-SE-CD-WIN7-P	1

Users with most Detections

	User Name	Count
1	Chuck	6
2	CS-SE-KM-1-12$	5
3	Demo	5
4	Ken	4
5	CS-SE-CC$	2
6	Christian_2	1
7	N/A	1

Files with most Detections

	File Name	Count
1	notepad.exe	6
2	iexplore.exe	5
3	powershell.exe	5
4	55d20a6f21d92b1abab894d1917d17fb6f0fd0adc2286074722864d271f202c1.exe	2
5		1
6	PING.EXE	1
7	net1.exe	1
8	pcinfo.exe	1
9	reg.exe	1
10	wevtutil.exe	1

Detections by Scenario

	Scenario	Description	Occurrences	On Machines	Unique SHA256s
1	drive_by_download	A browser created a process via shellcode.	6	2	1
2	known_malware	Metasploit's meterpreter server may have been loaded into a process.	6	2	2
3	credential_theft	LSASS process accessed from Powershell	4	2	1
4	suspicious_activity	PowerShell was run with a hidden window and encoded commands on the command line.	4	2	1
5	activity_prevented	This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was terminated.	2	1	1

« prev 1 2 3 next »

Detections by Severity

	Severity	Occurrences	On Machines	Unique SHA256s
1	High	10	3	5
2	Medium	8	3	4
3	Low	6	3	4

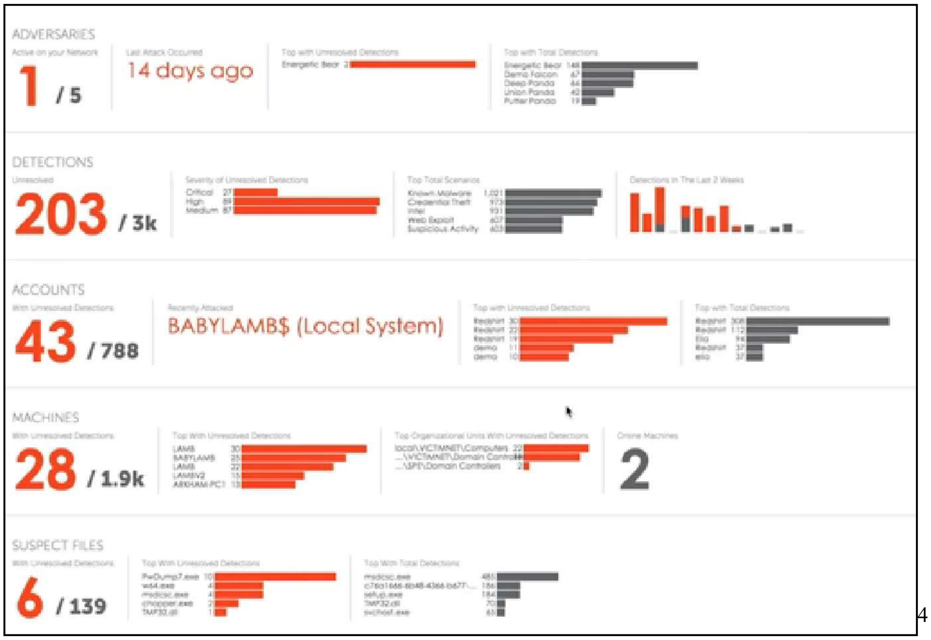
Detections by Host

	Host Name	Occurrences	Unique SHA256s
1	CS-SE-TG-W7-01	6	3
2	CS-SE-CC	4	3
3	CS-SE-KM-1-12	4	7
4	CS-SE-CD-WIN7-P	2	1

Detections by Hash

	MD5	SHA256	Occurrences	On Machines
1	c613e69c3b191bb02c7a191741a1d024	e285feeca968b3ca22017a64363eea5e69ccd519696671df523291b089597875	8	3
2	d378bffb70923139d6a4f546864aa61c	c4232ddd4d37b9c0884bd44d8476578c54d7f98d58945728e425736a6a07e102	6	2
3	852d67a27e454bd389fa7f02a8cbe23f	a8fdba9df15e41b6f5c69c79f66a26a9d48e174f9e7018a371600b866867dab8	4	2
4			2	1
5		55d20a6f21d92b1abab894d1917d17fb6f0fd0adc2286074722864d271f202c1	2	1
6	3b6928bc39e5530cead1e99269e7b1ee	0f084ccc40cbf7c3c7472ddad609b5fd31aacafa44e23f9ec7e9e2184713b986	2	1
7	5fb30fe90736c7fc77de637021b1ce7c	14262982a64551fde126339b22b993b6e4aed520e53dd882e67d887b6b66f942	2	1
8	8556041d4c2e616af49abbcb9d4ca9ee	9a6c3fd4cd0cc0d9156a3e7f0dfdef0d52ec329a057c17423f32aa6a3820deb8	2	1
9	9d0b3066fe3d1fd345e86bc7bcced9e4	4e66b857b7010db8d4e4e28d73eb81a99bd6915350bb9a63cd86671051b22f0e	2	1
10	dab04a7a5f67d2da07fc968eec76a5d2	0dd7d2a9e56ae356591c1792efb68a90fd76a7787e0b597fcbc4ef1fa514b601	2	1

[40]



[41]

86. Defendants have and continue to indirectly infringe one or more claims of the ’948 Patent by knowingly and intentionally inducing others, including CrowdStrike subsidiaries,

[39] *Id.*
[40] https://www.youtube.com/watch?v=IJARP_4vcHM
[41] https://www.youtube.com/watch?v=tgryLPiVGLE

customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '948 Accused Product (*e.g.*, products incorporating the Extended Detection and Response feature).

87. Defendants with knowledge that these products, or the use thereof, infringe the '948 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '948 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on their support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[42]

88. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing and maintaining those products, and provides technical support to users via the CrowdStrike support portal.[43]

89. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the "CrowdStrike Falcon agent" to be installed on individual endpoint computers.[44]

90. Defendants have induced and are currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with

[42] https://www.crowdstrike.com/products/crowdstrike-support/
[43] *Id.*
[44] https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/

the belief that there was a high probability that others, including end-users, infringe the ’948 Patent, but while remaining willfully blind to the infringement.

91. Taasera Licensing has suffered damages as a result of Defendants’ direct and indirect infringement of the ’948 Patent in an amount to be proved at trial.

92. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendants’ infringement of the ’948 Patent, for which there is no adequate remedy at law, unless Defendants’ infringement is enjoined by this Court.

COUNT V
(Infringement of the ’616 Patent)

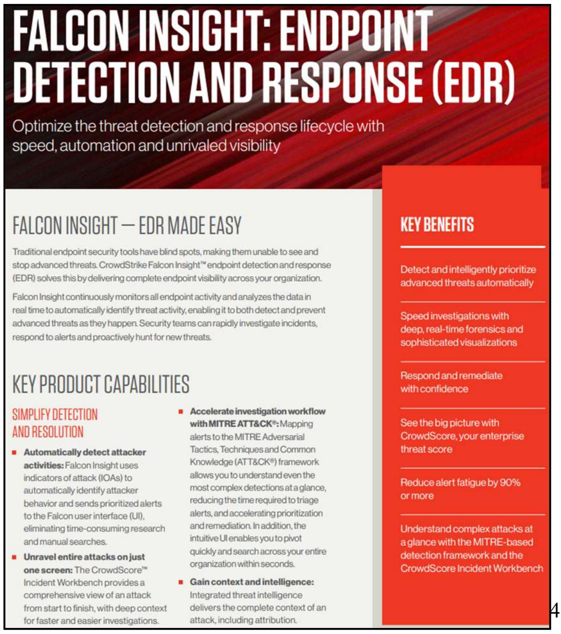
93. Paragraphs 1 through 35 are incorporated by reference as if fully set forth herein.

94. Defendants are not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’616 Patent.

95. Defendants have and continue to directly infringe at least claim 1 of the ’616 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’616 Patent. Such products incorporate the endpoint detection and vulnerability management features and include at least CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight (the “’616 Accused Products”) which practice a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of

the monitored device and the applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third-party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.

96. Every ’616 Accused Product practices a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) comprises cloud components and endpoint agents to provide operational integrity of a system.



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

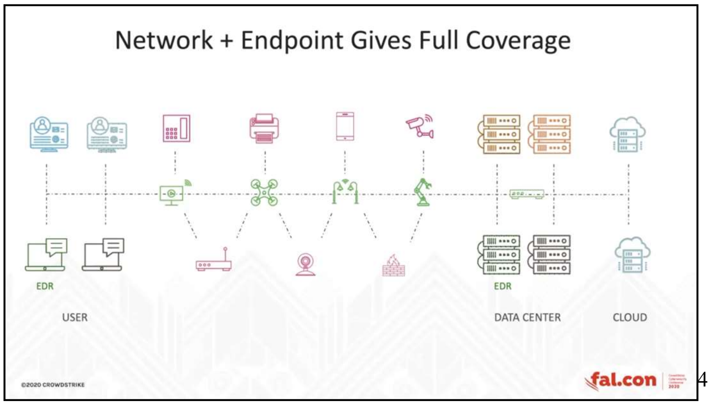
See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

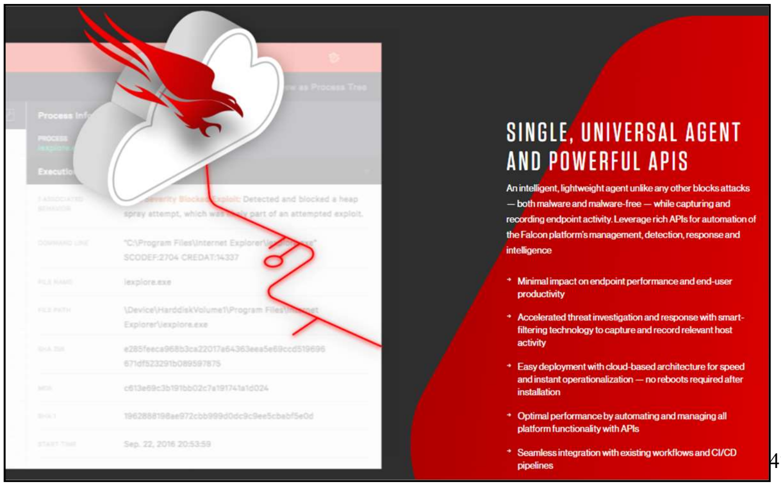
[45]

[45] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf



[46]

97. Every ’616 Accused Product practices sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime. For example, the endpoint agents send relevant host activity.



SINGLE, UNIVERSAL AGENT AND POWERFUL APIS

An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the Falcon platform's management, detection, response and intelligence

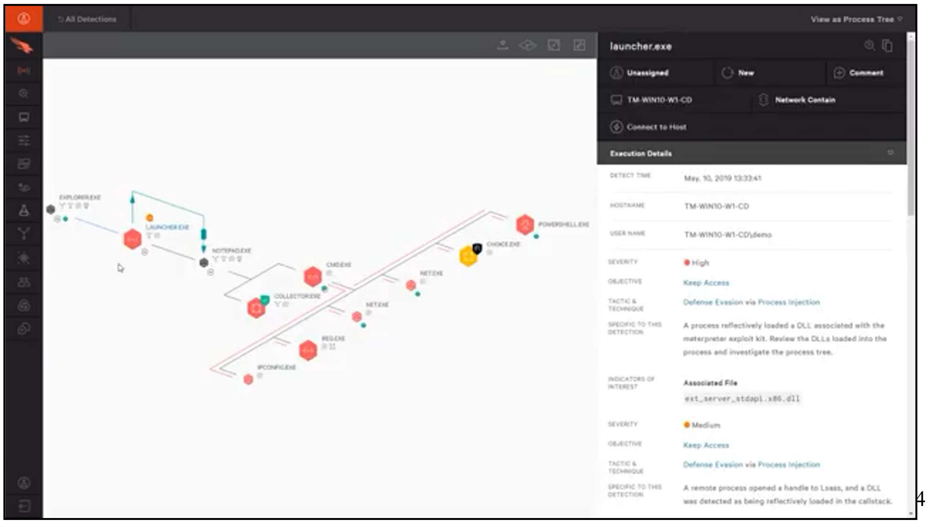
- Minimal impact on endpoint performance and end-user productivity
- Accelerated threat investigation and response with smart-filtering technology to capture and record relevant host activity
- Easy deployment with cloud-based architecture for speed and instant operationalization — no reboots required after installation
- Optimal performance by automating and managing all platform functionality with APIs
- Seamless integration with existing workflows and CI/CD pipelines

[47]

98. Every ’616 Accused Product practices receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime. For example, CrowdStrike Falcon Insight EDR

[46] https://www.crowdstrike.com/falcon/2020/videos/how-best-in-class-edr-and-ndr-deliver-world-class-xdr/
[47] https://www.crowdstrike.com/falcon-platform/

(with Falcon Agent) receives dynamic context including endpoint events and applications executing on the monitored device at runtime.



DETECT TIME May. 10, 2019 13:33:41

HOSTNAME TM-WIN10-W1-CD

USER NAME TM-WIN10-W1-CD\demo

SEVERITY High

OBJECTIVE Keep Access

TACTIC & TECHNIQUE Defense Evasion via Process Injection

SPECIFIC TO THIS DETECTION A process reflectively loaded a DLL associated with the meterpreter exploit kit. Review the DLLs loaded into the process and investigate the process tree.

INDICATORS OF INTEREST Associated File `ext_server_stdapi.x86.dll`

SEVERITY Medium

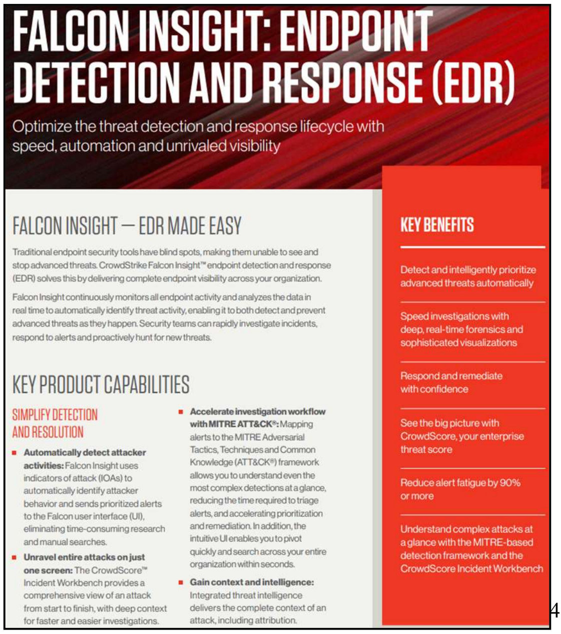
OBJECTIVE Keep Access

TACTIC & TECHNIQUE Defense Evasion via Process Injection

SPECIFIC TO THIS DETECTION A remote process opened a handle to Lsass, and a DLL was detected as being reflectively loaded in the callstack.

[48]

99. Every ’616 Accused Product practices analyzing, by the trust orchestration server, the received endpoint events. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) analyzes endpoint activity in real time to automatically identify threat activity.



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

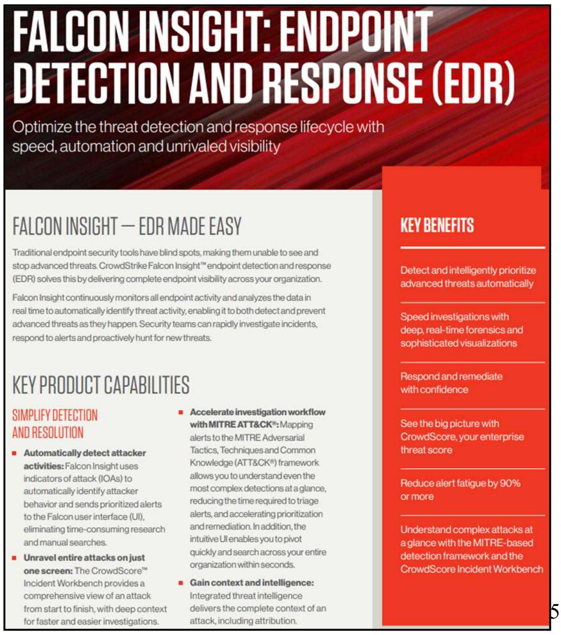
Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[49]

[48] https://www.youtube.com/watch?v=IJARP_4vcHM

[49] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

100. Every ’616 Accused Product practices receiving, by the trust orchestration server, third-party network endpoint assessments. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) receives MITRE ATT&CK data.



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

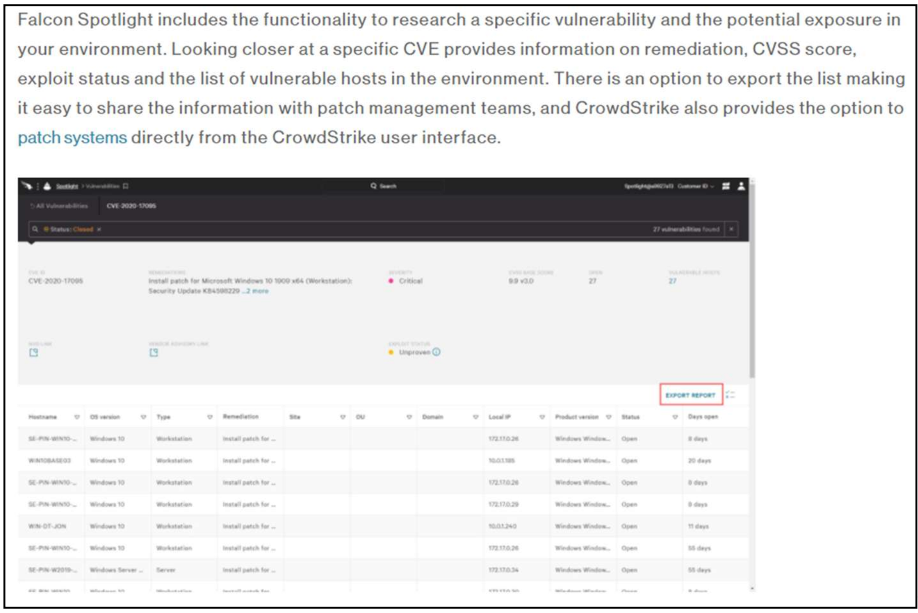
Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[50]

101. Every ’616 Accused Product practices generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) generates vulnerability data and assessed severity scores based at least in part on analyzing the third-party network endpoint assessments (*e.g.*, MITRE ATT&CK tactics and techniques).

[50] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

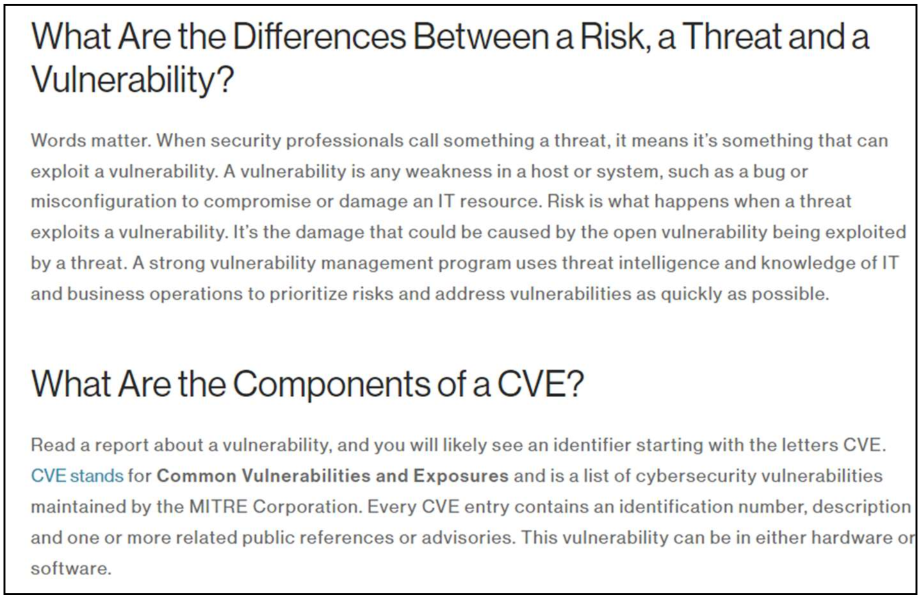


Falcon Spotlight includes the functionality to research a specific vulnerability and the potential exposure in your environment. Looking closer at a specific CVE provides information on remediation, CVSS score, exploit status and the list of vulnerable hosts in the environment. There is an option to export the list making it easy to share the information with patch management teams, and CrowdStrike also provides the option to patch systems directly from the CrowdStrike user interface.

CVE ID: CVE-2020-17095
REMEDIATIONS: Install patch for Microsoft Windows 10 1909 x64 (Workstation): Security Update KB4598229 ...2 more
SEVERITY: Critical
CVSS BASE SCORE: 9.9 v3.0
OPEN: 27
VULNERABLE HOSTS: 27
NVD LINK
VENDOR ADVISORY LINK
EXPLOIT STATUS: Unproven

Hostname	OS version	Type	Remediation	Site	OU	Domain	Local IP	Product version	Status	Days open
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.26	Windows Window...	Open	8 days
WIN10BASE03	Windows 10	Workstation	Install patch for ...				10.0.1.185	Windows Window...	Open	20 days
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.26	Windows Window...	Open	8 days
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.29	Windows Window...	Open	8 days
WIN-DT-JON	Windows 10	Workstation	Install patch for ...				10.0.1.240	Windows Window...	Open	11 days
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.26	Windows Window...	Open	55 days
SE-PIN-W2019-...	Windows Server ...	Server	Install patch for ...				172.17.0.34	Windows Window...	Open	55 days

[51]



What Are the Differences Between a Risk, a Threat and a Vulnerability?

Words matter. When security professionals call something a threat, it means it's something that can exploit a vulnerability. A vulnerability is any weakness in a host or system, such as a bug or misconfiguration to compromise or damage an IT resource. Risk is what happens when a threat exploits a vulnerability. It's the damage that could be caused by the open vulnerability being exploited by a threat. A strong vulnerability management program uses threat intelligence and knowledge of IT and business operations to prioritize risks and address vulnerabilities as quickly as possible.

What Are the Components of a CVE?

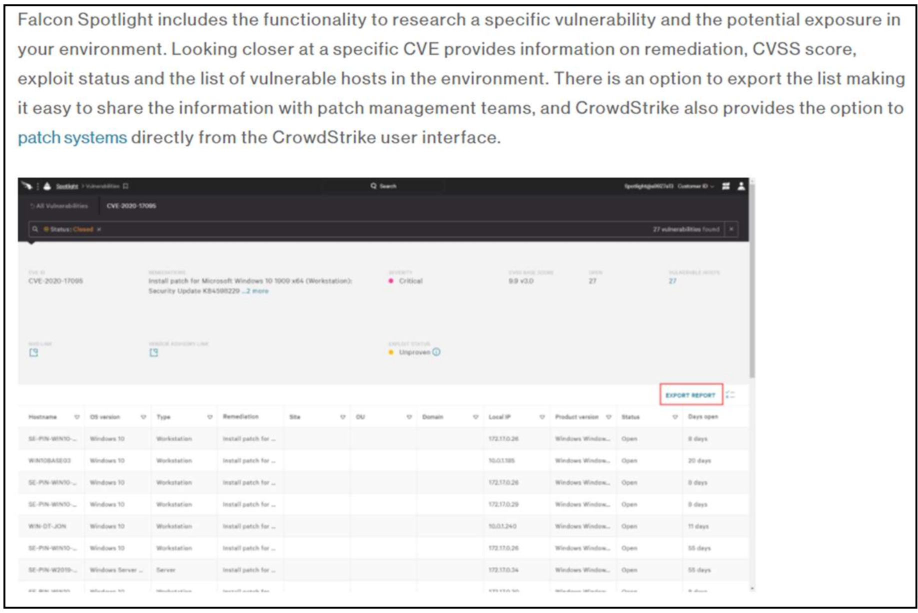
Read a report about a vulnerability, and you will likely see an identifier starting with the letters CVE. CVE stands for **Common Vulnerabilities and Exposures** and is a list of cybersecurity vulnerabilities maintained by the MITRE Corporation. Every CVE entry contains an identification number, description and one or more related public references or advisories. This vulnerability can be in either hardware or software.

[52]

102. Every ’616 Accused Product practices correlating, by the trust orchestration server, the received endpoint events and the generated temporal events. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) correlates the received endpoint events and the generated temporal events (*e.g.*, vulnerability data and assessed severity scores).

[51] https://www.crowdstrike.com/blog/tech-center/falcon-spotlight-for-vulnerability-management/

[52] https://www.crowdstrike.com/blog/how-to-stay-ahead-of-common-vulnerabilities-and-exposures-in-your-environment/



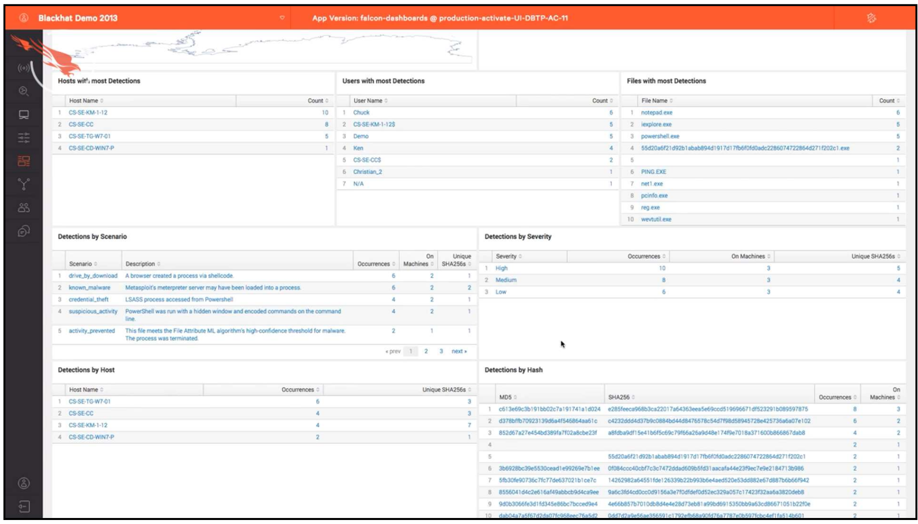
Falcon Spotlight includes the functionality to research a specific vulnerability and the potential exposure in your environment. Looking closer at a specific CVE provides information on remediation, CVSS score, exploit status and the list of vulnerable hosts in the environment. There is an option to export the list making it easy to share the information with patch management teams, and CrowdStrike also provides the option to patch systems directly from the CrowdStrike user interface.

CVE ID: CVE-2020-17095
REMEDIATIONS: Install patch for Microsoft Windows 10 1909 x64 (Workstation): Security Update KB4586229 ...2 more
SEVERITY: Critical
CVSS BASE SCORE: 9.9 v3.0
OPEN: 27
VULNERABLE HOSTS: 27
NVD LINK
VENDOR ADVISORY LINK
EXPLOIT STATUS: Unproven

Hostname	OS version	Type	Remediation	Site	OU	Domain	Local IP	Product version	Status	Days open
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.26	Windows Window...	Open	8 days
WIN10BASE03	Windows 10	Workstation	Install patch for ...				10.0.1.185	Windows Window...	Open	20 days
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.26	Windows Window...	Open	8 days
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.29	Windows Window...	Open	8 days
WIN-DT-JON	Windows 10	Workstation	Install patch for ...				10.0.1.240	Windows Window...	Open	11 days
SE-PIN-WIN10-...	Windows 10	Workstation	Install patch for ...				172.17.0.26	Windows Window...	Open	55 days
SE-PIN-W2019-...	Windows Server ...	Server	Install patch for ...				172.17.0.34	Windows Window...	Open	55 days

[53]

103. Every ’616 Accused Product practices generating, by the trust orchestration server, an integrity profile for the system. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) generates an integrity profile for the system in displaying detected MITRE ATT&CK tactics and techniques.



Blackhat Demo 2013
App Version: falcon-dashboards @ production-activate-UI-DBTP-AC-11

Hosts wit'ı most Detections

	Host Name	Count
1	CS-SE-KM-1-12	10
2	CS-SE-CC	8
3	CS-SE-TG-W7-01	5
4	CS-SE-CD-WIN7-P	1

Users with most Detections

	User Name	Count
1	Chuck	6
2	CS-SE-KM-1-12$	5
3	Demo	5
4	Ken	4
5	CS-SE-CC$	2
6	Christian_2	1
7	N/A	1

Files with most Detections

	File Name	Count
1	notepad.exe	6
2	iexplore.exe	5
3	powershell.exe	5
4	55d20a6f21d92b1abab894d1917d17fb6f0fd0adc2286074722864d271f202c1.exe	2
5		1
6	PING.EXE	1
7	net1.exe	1
8	pcinfo.exe	1
9	reg.exe	1
10	wevtutil.exe	1

Detections by Scenario

	Scenario	Description	Occurrences	On Machines	Unique SHA256s
1	drive_by_download	A browser created a process via shellcode.	6	2	1
2	known_malware	Metasploit's meterpreter server may have been loaded into a process.	6	2	2
3	credential_theft	LSASS process accessed from Powershell	4	2	1
4	suspicious_activity	PowerShell was run with a hidden window and encoded commands on the command line.	4	2	1
5	activity_prevented	This file meets the File Attribute ML algorithm's high-confidence threshold for malware. The process was terminated.	2	1	1

« prev 1 2 3 next »

Detections by Severity

	Severity	Occurrences	On Machines	Unique SHA256s
1	High	10	3	5
2	Medium	8	3	4
3	Low	6	3	4

Detections by Host

	Host Name	Occurrences	Unique SHA256s
1	CS-SE-TG-W7-01	6	3
2	CS-SE-CC	4	3
3	CS-SE-KM-1-12	4	7
4	CS-SE-CD-WIN7-P	2	1

Detections by Hash

	MD5	SHA256	Occurrences	On Machines
1	c613e69c3b191bb02c7a191741a1d024	e285feeca968b3ca22017a64363eea5e69ccd519696671df523291b089597875	8	3
2	d378bffb70923139d6a4f546864aa61c	c4232ddd4d37b9c0884bd44d8476578c54d7f98d58945728e425736a6a07e102	6	2
3	852d67a27e454bd389fa7f02a8cbe23f	a8fdba9df15e41b6f5c69c79f66a26a9d48e174f9e7018a371600b866867dab8	4	2
4			2	1
5		55d20a6f21d92b1abab894d1917d17fb6f0fd0adc2286074722864d271f202c1	2	1
6	3b6928bc39e5530cead1e99269e7b1ee	0f084ccc40cbf7c3c7472ddad609b5fd31aacafa44e23f9ec7e9e2184713b986	2	1
7	5fb30fe90736c7fc77de637021b1ce7c	14262982a64551fde126339b22b993b6e4aed520e53dd882e67d887b6b66f942	2	1
8	8556041d4c2e616af49abbcb9d4ca9ee	9a6c3fd4cd0cc0d9156a3e7f0dfdef0d52ec329a057c17423f32aa6a3820deb8	2	1
9	9d0b3066fe3d1fd345e86bc7bcced9e4	4e66b857b7010db8d4e4e28d73eb81a99bd6915350bb9a63cd86671051b22f0e	2	1
10	dab04a7a5f67d2da07fc968eec76a5d2	0dd7d2a9e56ae356591c1792efb68a90fd76a7787e0b597fcbc4ef1fa514b601	2	1

[54]

[53] https://www.crowdstrike.com/blog/tech-center/falcon-spotlight-for-vulnerability-management/
[54] https://www.youtube.com/watch?v=odGDYzQbe80&t=1s

104. Defendants have and continue to indirectly infringe one or more claims of the ’616 Patent by knowingly and intentionally inducing others, including CrowdStrike subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’616 Accused Products (*e.g.*, products incorporating the Vulnerability Management feature).

105. Defendants with knowledge that these products, or the use thereof, infringe the ’616 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continue to knowingly and intentionally induce, direct infringement of the ’616 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on their support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[55]

106. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing and maintaining those products, and provides technical support to users via the CrowdStrike support portal.[56]

107. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the “CrowdStrike Falcon agent” to be installed on individual endpoint computers.[57]

[55] https://www.crowdstrike.com/products/crowdstrike-support/

[56] *Id.*

[57] https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/

108. Defendants have induced and are currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’616 Patent, but while remaining willfully blind to the infringement.

109. Taasera Licensing has suffered damages as a result of Defendants’ direct and indirect infringement of the ’616 Patent in an amount to be proved at trial.

110. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendants’ infringement of the ’616 Patent, for which there is no adequate remedy at law, unless Defendants’ infringement is enjoined by this Court.

COUNT VI
(Infringement of the ’997 Patent)

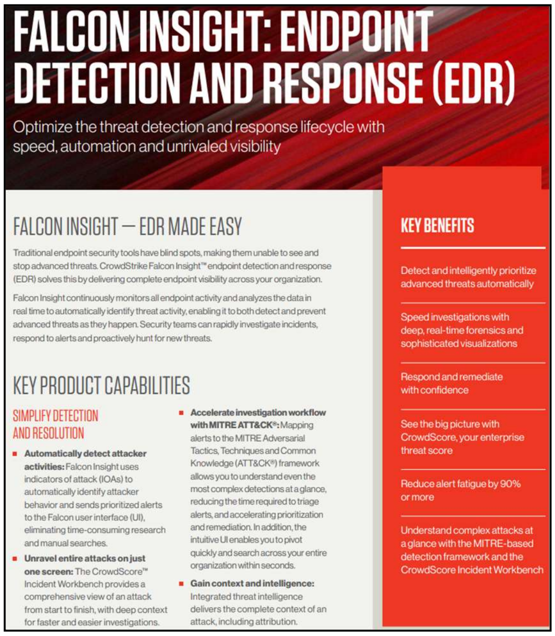
111. Paragraphs 1 through 35 are incorporated by reference as if fully set forth herein.

112. Defendants are not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’997 Patent.

113. Defendants have and continue to directly infringe at least claim 21 of the ’997 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’997 Patent. Such products include at least CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight (the “’997 Accused Products”) which is a system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software services provided by an operating system on the endpoint configured to monitor a plurality of operating conditions identified in the

plurality of policies; and one or more hardware processors at the computing system configured to: receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services, determining a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system.

114. Every ’997 Accused Product is a system for controlling the operation of an endpoint. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight controls the operation of an endpoint.



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

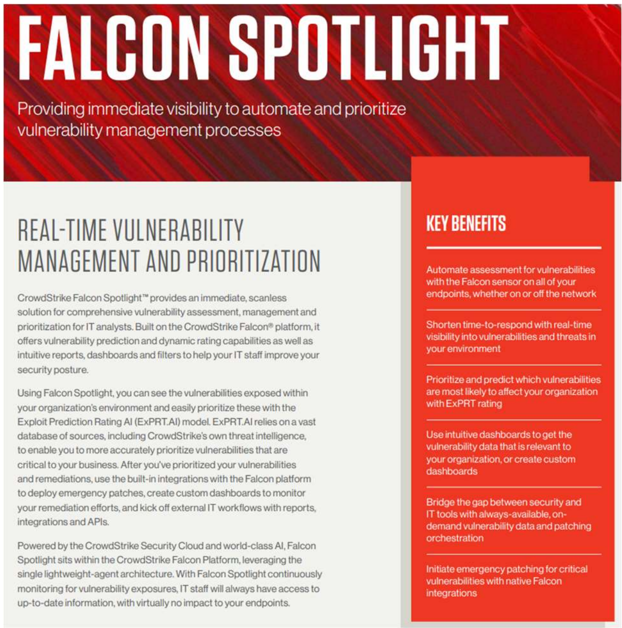
Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[58]



FALCON SPOTLIGHT

Providing immediate visibility to automate and prioritize vulnerability management processes

REAL-TIME VULNERABILITY MANAGEMENT AND PRIORITIZATION

CrowdStrike Falcon Spotlight™ provides an immediate, scanless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. Built on the CrowdStrike Falcon® platform, it offers vulnerability prediction and dynamic rating capabilities as well as intuitive reports, dashboards and filters to help your IT staff improve your security posture.

Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.

Powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight sits within the CrowdStrike Falcon Platform, leveraging the single lightweight-agent architecture. With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.

KEY BENEFITS

Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network

Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment

Prioritize and predict which vulnerabilities are most likely to affect your organization with ExPRT rating

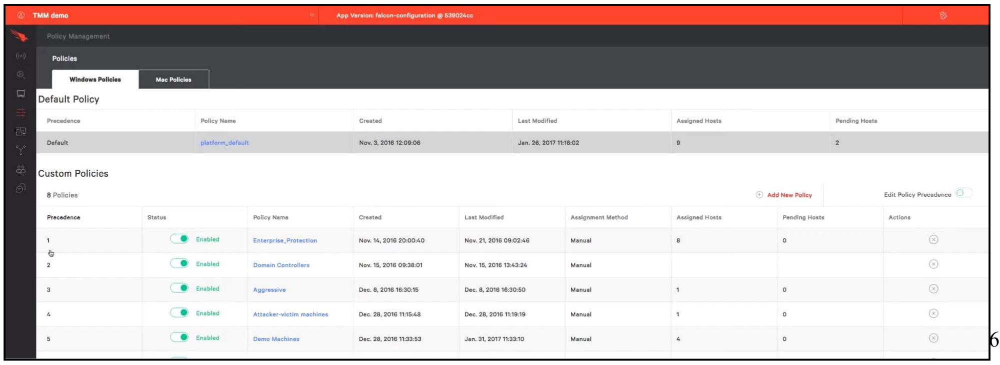
Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards

Bridge the gap between security and IT tools with always-available, on-demand vulnerability data and patching orchestration

Initiate emergency patching for critical vulnerabilities with native Falcon integrations

[59]

115. Every '997 Accused Product comprises a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies, and a data store, at the computing system, that contains the plurality of policies. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) allows configuration of a plurality of policies at a system remote from the endpoint through a provided user interface which are stored in a data store.



Default Policy

Precedence	Policy Name	Created	Last Modified	Assigned Hosts	Pending Hosts
Default	platform_default	Nov. 3, 2016 12:09:06	Jan. 26, 2017 11:16:02	9	2

Custom Policies

8 Policies

Precedence	Status	Policy Name	Created	Last Modified	Assignment Method	Assigned Hosts	Pending Hosts	Actions
1	Enabled	Enterprise_Protection	Nov. 14, 2016 20:00:40	Nov. 21, 2016 09:02:46	Manual	8	0	⊗
2	Enabled	Domain Controllers	Nov. 15, 2016 09:38:01	Nov. 15, 2016 13:43:24	Manual			⊗
3	Enabled	Aggressive	Dec. 8, 2016 16:30:15	Dec. 8, 2016 16:30:50	Manual	1	0	⊗
4	Enabled	Attacker-victim machines	Dec. 28, 2016 11:15:48	Dec. 28, 2016 11:19:19	Manual	1	0	⊗
5	Enabled	Demo Machines	Dec. 28, 2016 11:33:53	Jan. 31, 2017 11:33:10	Manual	4	0	⊗

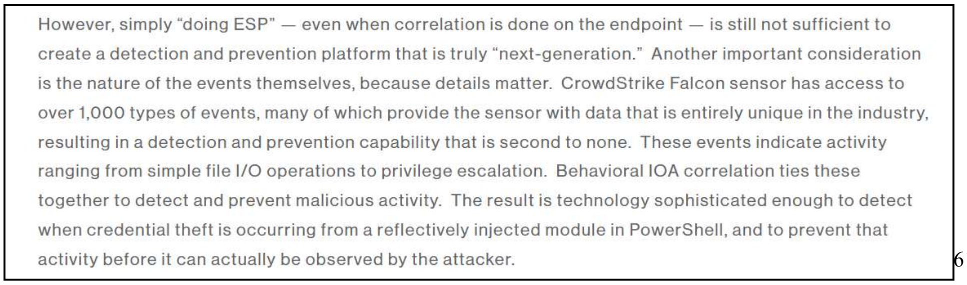
[60]

[58] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

[59] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-spotlight-data-sheet.pdf

[60] https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/

116. Every ’997 Accused Product comprises one or more software services provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) comprises the Falcon sensor that detects file I/O operations, privilege escalation, and behavioral IOAs identified in the plurality of policies.

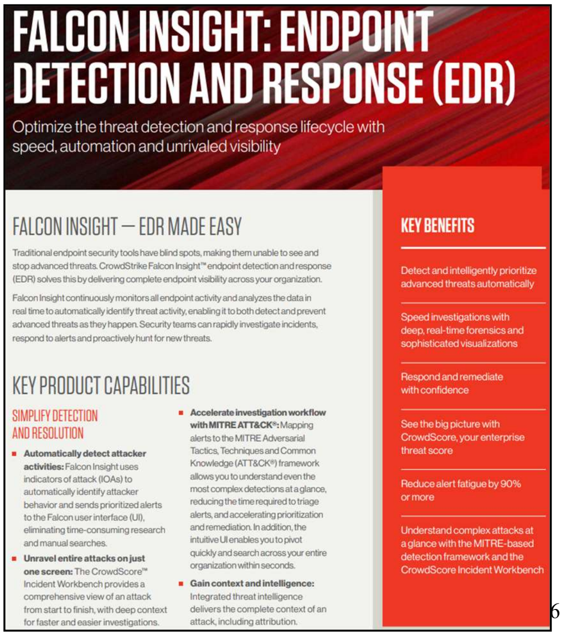


However, simply “doing ESP” — even when correlation is done on the endpoint — is still not sufficient to create a detection and prevention platform that is truly “next-generation.” Another important consideration is the nature of the events themselves, because details matter. CrowdStrike Falcon sensor has access to over 1,000 types of events, many of which provide the sensor with data that is entirely unique in the industry, resulting in a detection and prevention capability that is second to none. These events indicate activity ranging from simple file I/O operations to privilege escalation. Behavioral IOA correlation ties these together to detect and prevent malicious activity. The result is technology sophisticated enough to detect when credential theft is occurring from a reflectively injected module in PowerShell, and to prevent that activity before it can actually be observed by the attacker.[61]

117. Every ’997 Accused Product receives, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) detects and receives alerts for suspicious endpoint activity gathered by the Falcon sensor.[62]

[61] https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/

[62] https://www.youtube.com/watch?v=VuiPG1PiMsM



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

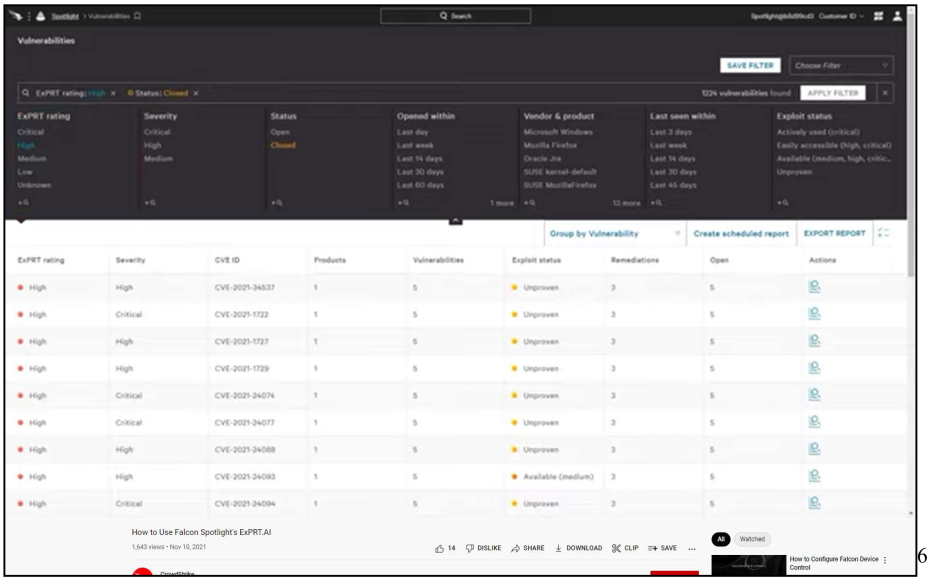
See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[63]

118. Every '997 Accused Product determines a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight determines a compliance state of the endpoint based on the exploit status and a plurality of compliance policies.



Vulnerabilities

ExPRT rating: High × Status: Closed ×

1224 vulnerabilities found

ExPRT rating	Severity	Status	Opened within	Vendor & product	Last seen within	Exploit status
Critical	Critical	Open	Last day	Microsoft Windows	Last 3 days	Actively used (critical)
High	High	Closed	Last week	Mozilla Firefox	Last week	Easily accessible (high, critical)
Medium	Medium		Last 14 days	Oracle Jre	Last 14 days	Available (medium, high, critic...
Low			Last 30 days	SUSE kernel-default	Last 30 days	Unproven
Unknown			Last 60 days	SUSE MozillaFirefox	Last 45 days	
			1 more	13 more		

ExPRT rating	Severity	CVE ID	Products	Vulnerabilities	Exploit status	Remediations	Open	Actions
● High	High	CVE-2021-34537	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-1722	1	5	● Unproven	3	5	
● High	High	CVE-2021-1727	1	5	● Unproven	3	5	
● High	High	CVE-2021-1729	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-24074	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-24077	1	5	● Unproven	3	5	
● High	High	CVE-2021-24088	1	5	● Unproven	3	5	
● High	High	CVE-2021-24093	1	5	● Available (medium)	3	5	
● High	Critical	CVE-2021-24094	1	5	● Unproven	3	5	

How to Use Falcon Spotlight's ExPRT.AI

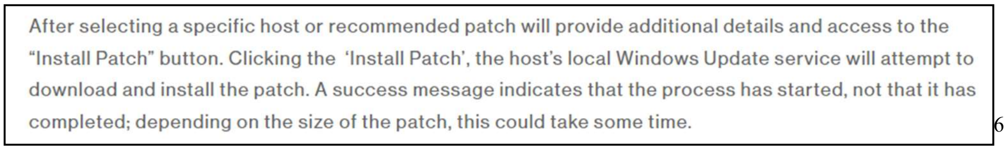
1,643 views • Nov 10, 2021

[64]

[63] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

[64] https://www.youtube.com/watch?v=P1qOGCeEYK8

119. Every ’997 Accused Product practices initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a hardware processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight provides an “Install Patch” button when a patch is required. The patch is installed by the endpoint.[65]



After selecting a specific host or recommended patch will provide additional details and access to the “Install Patch” button. Clicking the ‘Install Patch’, the host’s local Windows Update service will attempt to download and install the patch. A success message indicates that the process has started, not that it has completed; depending on the size of the patch, this could take some time.[66]

120. Defendants have and continue to indirectly infringe one or more claims of the ’997 Patent by knowingly and intentionally inducing others, including CrowdStrike subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the ’997 Accused Products (*e.g.*, products incorporating the Vulnerability Management feature).

121. Defendants with knowledge that these products, or the use thereof, infringe the ’997 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continue to knowingly and intentionally induce, direct infringement of the ’997 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and

[65] *Id.*

[66] https://www.crowdstrike.com/blog/tech-center/emergency-patching/

installation manuals on their support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[67]

122. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing and maintaining those products, and provides technical support to users via the CrowdStrike support portal.[68]

123. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the "CrowdStrike Falcon agent" to be installed on individual endpoint computers.[69]

124. Defendants have induced and are currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '997 Patent, but while remaining willfully blind to the infringement.

125. Taasera Licensing has suffered damages as a result of Defendants' direct and indirect infringement of the '997 Patent in an amount to be proved at trial.

126. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendants' infringement of the '997 Patent, for which there is no adequate remedy at law, unless Defendants' infringement is enjoined by this Court.

COUNT VII
(Infringement of the '918 Patent)

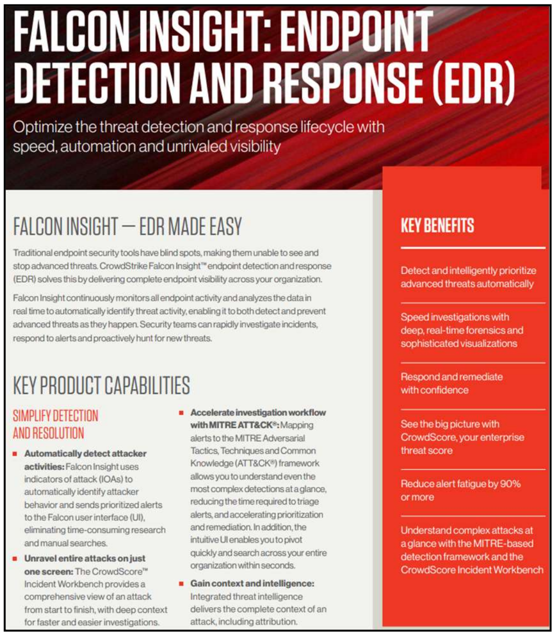
127. Paragraphs 1 through 35 are incorporated by reference as if fully set forth herein.

[67] https://www.crowdstrike.com/products/crowdstrike-support/
[68] *Id.*
[69] https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/

128. Defendants are not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’918 Patent.

129. Defendants have and continues to directly infringe at least claim 1 of the ’918 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’918 Patent. Such products include at least CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight (the “’918 Accused Products”) which comprise a system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to receive, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint, determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store, and authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.

130. Every ’918 Accused Product comprises a system for controlling the operation of an endpoint. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) controls the operation of an endpoint.



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

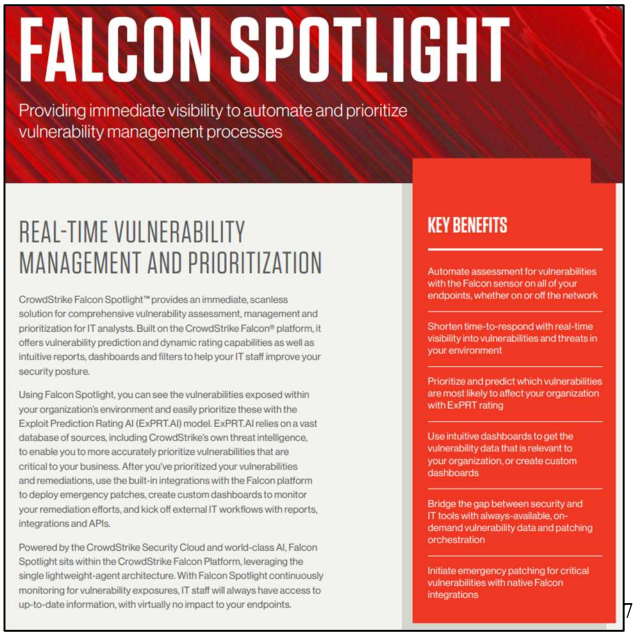
Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[70]



FALCON SPOTLIGHT

Providing immediate visibility to automate and prioritize vulnerability management processes

REAL-TIME VULNERABILITY MANAGEMENT AND PRIORITIZATION

CrowdStrike Falcon Spotlight™ provides an immediate, scanless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. Built on the CrowdStrike Falcon® platform, it offers vulnerability prediction and dynamic rating capabilities as well as intuitive reports, dashboards and filters to help your IT staff improve your security posture.

Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.

Powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight sits within the CrowdStrike Falcon Platform, leveraging the single lightweight-agent architecture. With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.

KEY BENEFITS

Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network

Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment

Prioritize and predict which vulnerabilities are most likely to affect your organization with ExPRT rating

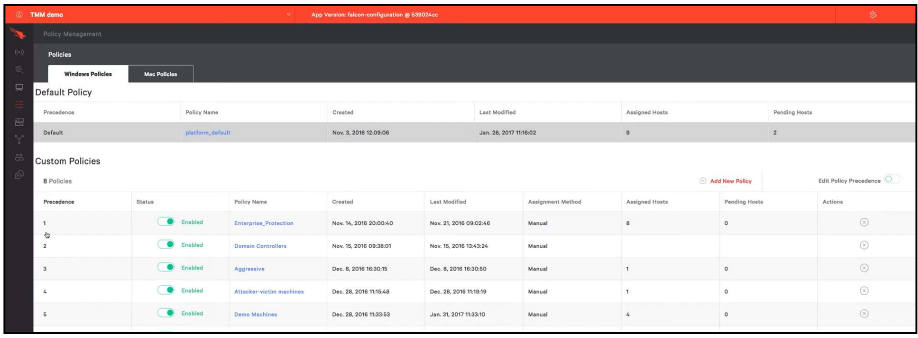
Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards

Bridge the gap between security and IT tools with always-available, on-demand vulnerability data and patching orchestration

Initiate emergency patching for critical vulnerabilities with native Falcon integrations

[71]

131. Every ’918 Accused Product comprises a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies, and a data store, at the computing system, that contains the plurality of policies. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) comprises a user interface that allows configuration of a plurality of policies at a system remote from the endpoint which are stored in the CrowdStrike data store.



TMM demo

App Version: falcon-configuration @ 539024cc

Policy Management

Policies

Default Policy

Precedence	Policy Name	Created	Last Modified	Assigned Hosts	Pending Hosts
Default	platform_default	Nov. 3, 2016 12:09:06	Jan. 26, 2017 11:16:02	9	2

Custom Policies

8 Policies

Precedence	Status	Policy Name	Created	Last Modified	Assignment Method	Assigned Hosts	Pending Hosts	Actions
1	Enabled	Enterprise_Protection	Nov. 14, 2016 20:00:40	Nov. 21, 2016 09:02:46	Manual	8	0	⊗
2	Enabled	Domain Controllers	Nov. 15, 2016 09:38:01	Nov. 15, 2016 13:43:24	Manual			⊗
3	Enabled	Aggressive	Dec. 8, 2016 16:30:15	Dec. 8, 2016 16:30:50	Manual	1	0	⊗
4	Enabled	Attacker-victim machines	Dec. 28, 2016 11:15:48	Dec. 28, 2016 11:19:19	Manual	1	0	⊗
5	Enabled	Demo Machines	Dec. 28, 2016 11:33:53	Jan. 31, 2017 11:33:10	Manual	4	0	⊗

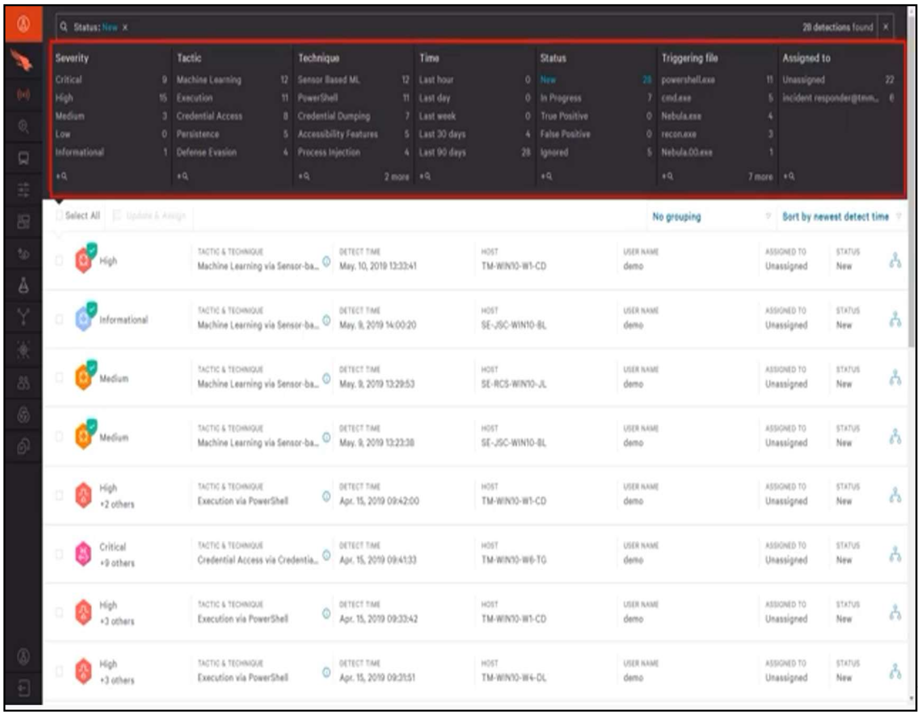
[72]

[70] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

[71] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-spotlight-data-sheet.pdf

[72] https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/

132. Every ’918 Accused Product comprises one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) comprises the Falcon sensor that detects file I/O operations, privilege escalation, and behavioral IOAs identified in the plurality of policies.



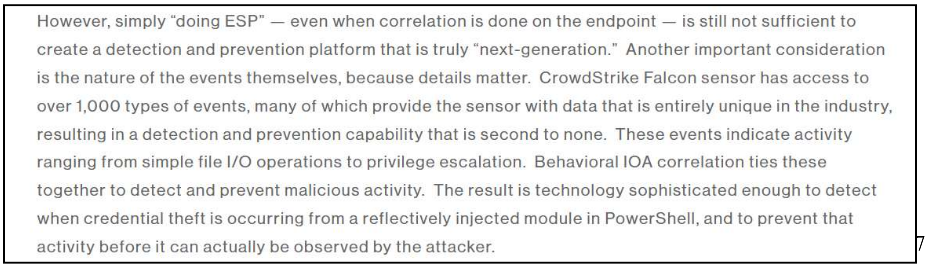
Status: New ×   28 detections found ×

Severity		Tactic		Technique		Time		Status		Triggering file		Assigned to	
Critical	9	Machine Learning	12	Sensor Based ML	12	Last hour	0	New	28	powershell.exe	11	Unassigned	22
High	15	Execution	11	PowerShell	11	Last day	0	In Progress	7	cmd.exe	5	incident responder@tmm...	6
Medium	3	Credential Access	8	Credential Dumping	7	Last week	0	True Positive	0	Nebula.exe	4		
Low	0	Persistence	5	Accessibility Features	5	Last 30 days	4	False Positive	0	recon.exe	3		
Informational	1	Defense Evasion	4	Process Injection	4	Last 90 days	28	Ignored	5	Nebula.00.exe	1		
+Q		+Q		+Q	2 more	+Q		+Q		+Q	7 more	+Q	

□ Select All   Update & Assign   No grouping   Sort by newest detect time

	TACTIC & TECHNIQUE	DETECT TIME	HOST	USER NAME	ASSIGNED TO	STATUS
High	Machine Learning via Sensor-ba...	May. 10, 2019 13:33:41	TM-WIN10-W1-CD	demo	Unassigned	New
Informational	Machine Learning via Sensor-ba...	May. 9, 2019 14:00:20	SE-JSC-WIN10-BL	demo	Unassigned	New
Medium	Machine Learning via Sensor-ba...	May. 9, 2019 13:29:53	SE-RCS-WIN10-JL	demo	Unassigned	New
Medium	Machine Learning via Sensor-ba...	May. 9, 2019 13:23:38	SE-JSC-WIN10-BL	demo	Unassigned	New
High +2 others	Execution via PowerShell	Apr. 15, 2019 09:42:00	TM-WIN10-W1-CD	demo	Unassigned	New
Critical +9 others	Credential Access via Credentia...	Apr. 15, 2019 09:41:33	TM-WIN10-W6-TG	demo	Unassigned	New
High +3 others	Execution via PowerShell	Apr. 15, 2019 09:33:42	TM-WIN10-W1-CD	demo	Unassigned	New
High +3 others	Execution via PowerShell	Apr. 15, 2019 09:31:51	TM-WIN10-W4-DL	demo	Unassigned	New

[73]



However, simply “doing ESP” — even when correlation is done on the endpoint — is still not sufficient to create a detection and prevention platform that is truly “next-generation.” Another important consideration is the nature of the events themselves, because details matter. CrowdStrike Falcon sensor has access to over 1,000 types of events, many of which provide the sensor with data that is entirely unique in the industry, resulting in a detection and prevention capability that is second to none. These events indicate activity ranging from simple file I/O operations to privilege escalation. Behavioral IOA correlation ties these together to detect and prevent malicious activity. The result is technology sophisticated enough to detect when credential theft is occurring from a reflectively injected module in PowerShell, and to prevent that activity before it can actually be observed by the attacker.

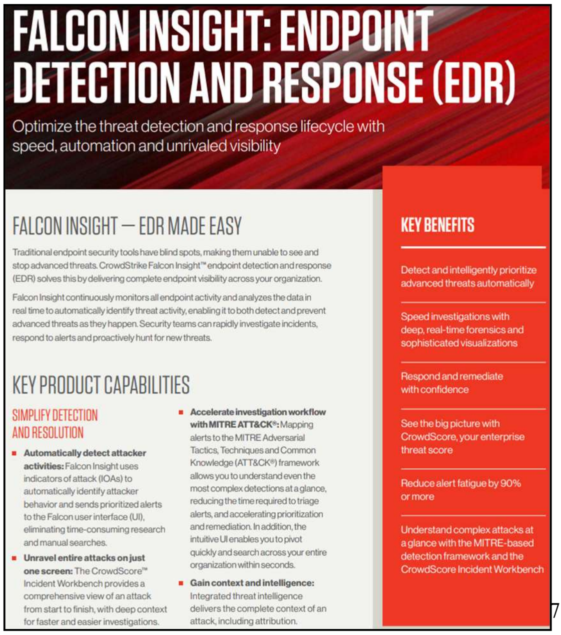
[74]

133. Every ’918 Accused Product receives, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one

[73] https://www.youtube.com/watch?v=VuiPG1PiMsM

[74] https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon/

or more software services on the endpoint, and user information that identified a user of the endpoint. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) detects and receives alerts for suspicious endpoint activity gathered by the Falcon sensor.[75]



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

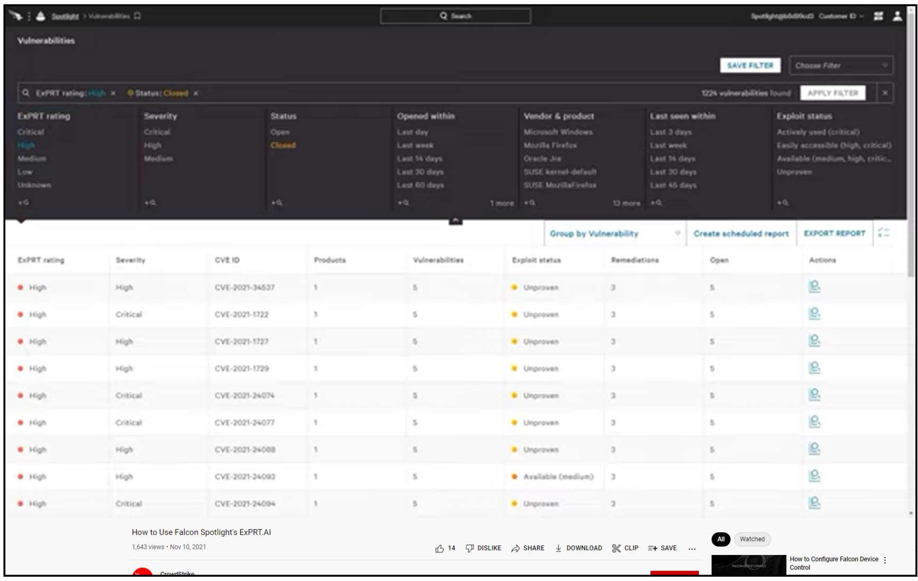
Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[76]

134. Every '918 Accused Product determines, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) with Falcon Spotlight determines a compliance state of the endpoint based on the exploit status and a plurality of compliance policies.

[75] https://www.youtube.com/watch?v=VuiPG1PiMsM

[76] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

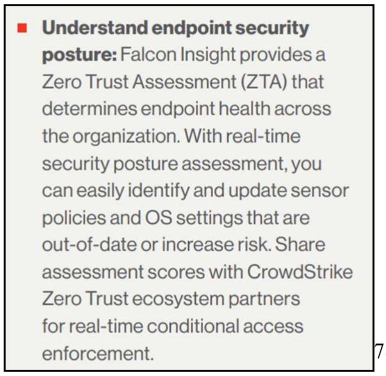


ExPRT rating	Severity	CVE ID	Products	Vulnerabilities	Exploit status	Remediations	Open	Actions
● High	High	CVE-2021-34537	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-1722	1	5	● Unproven	3	5	
● High	High	CVE-2021-1727	1	5	● Unproven	3	5	
● High	High	CVE-2021-1729	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-24074	1	5	● Unproven	3	5	
● High	Critical	CVE-2021-24077	1	5	● Unproven	3	5	
● High	High	CVE-2021-24088	1	5	● Unproven	3	5	
● High	High	CVE-2021-24093	1	5	● Available (medium)	3	5	
● High	Critical	CVE-2021-24094	1	5	● Unproven	3	5	

How to Use Falcon Spotlight's ExPRT.AI
1,643 views • Nov 10, 2021
CrowdStrike
14
DISLIKE
SHARE
DOWNLOAD
CLIP
SAVE
All
Watched
How to Configure Falcon Device Control

[77]

135. Every ’918 Accused Product authorizes access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent)’s Zero Trust Assessment authorizes access by the endpoint to a computing resource on the network (*e.g.*, dynamic conditional access) in response to the compliance state (*e.g.*, based on device health and compliance checks).

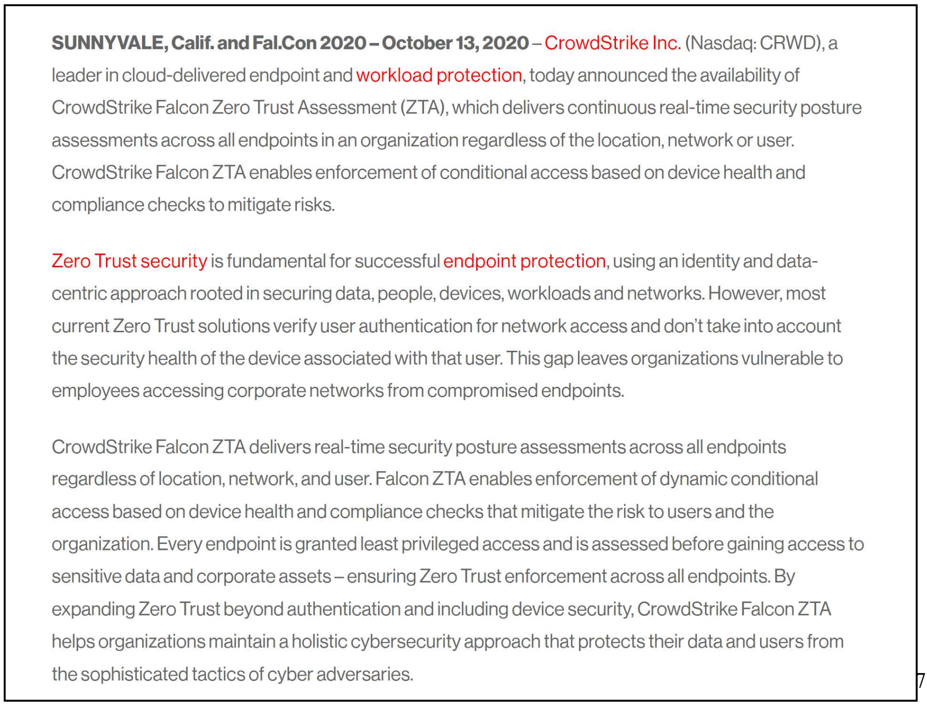


- **Understand endpoint security posture:** Falcon Insight provides a Zero Trust Assessment (ZTA) that determines endpoint health across the organization. With real-time security posture assessment, you can easily identify and update sensor policies and OS settings that are out-of-date or increase risk. Share assessment scores with CrowdStrike Zero Trust ecosystem partners for real-time conditional access enforcement.

[78]

[77] https://www.youtube.com/watch?v=P1qOGCeEYK8

[78] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf



SUNNYVALE, Calif. and Fal.Con 2020 – October 13, 2020 – CrowdStrike Inc. (Nasdaq: CRWD), a leader in cloud-delivered endpoint and workload protection, today announced the availability of CrowdStrike Falcon Zero Trust Assessment (ZTA), which delivers continuous real-time security posture assessments across all endpoints in an organization regardless of the location, network or user. CrowdStrike Falcon ZTA enables enforcement of conditional access based on device health and compliance checks to mitigate risks.

Zero Trust security is fundamental for successful endpoint protection, using an identity and data-centric approach rooted in securing data, people, devices, workloads and networks. However, most current Zero Trust solutions verify user authentication for network access and don't take into account the security health of the device associated with that user. This gap leaves organizations vulnerable to employees accessing corporate networks from compromised endpoints.

CrowdStrike Falcon ZTA delivers real-time security posture assessments across all endpoints regardless of location, network, and user. Falcon ZTA enables enforcement of dynamic conditional access based on device health and compliance checks that mitigate the risk to users and the organization. Every endpoint is granted least privileged access and is assessed before gaining access to sensitive data and corporate assets – ensuring Zero Trust enforcement across all endpoints. By expanding Zero Trust beyond authentication and including device security, CrowdStrike Falcon ZTA helps organizations maintain a holistic cybersecurity approach that protects their data and users from the sophisticated tactics of cyber adversaries.

[79]

136. Defendants have and continue to indirectly infringe one or more claims of the '918 Patent by knowingly and intentionally inducing others, including CrowdStrike subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the '918 Accused Product (*e.g.*, products incorporating the Vulnerability Management feature).

137. Defendants with knowledge that these products, or the use thereof, infringe the '918 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continue to knowingly and intentionally induce, direct infringement of the '918 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and

[79] https://www.youtube.com/watch?v=P1qOGCeEYK8

installation manuals on their support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[80]

138. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing and maintaining those products, and provides technical support to users via the CrowdStrike support portal.[81]

139. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the "CrowdStrike Falcon agent" to be installed on individual endpoint computers.[82]

140. Defendants have induced and are currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '918 Patent, but while remaining willfully blind to the infringement.

141. Taasera Licensing has suffered damages as a result of Defendants' direct and indirect infringement of the '918 Patent in an amount to be proved at trial.

142. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendants' infringement of the '918 Patent, for which there is no adequate remedy at law, unless Defendants' infringement is enjoined by this Court.

COUNT VIII
(Infringement of the '517 Patent)

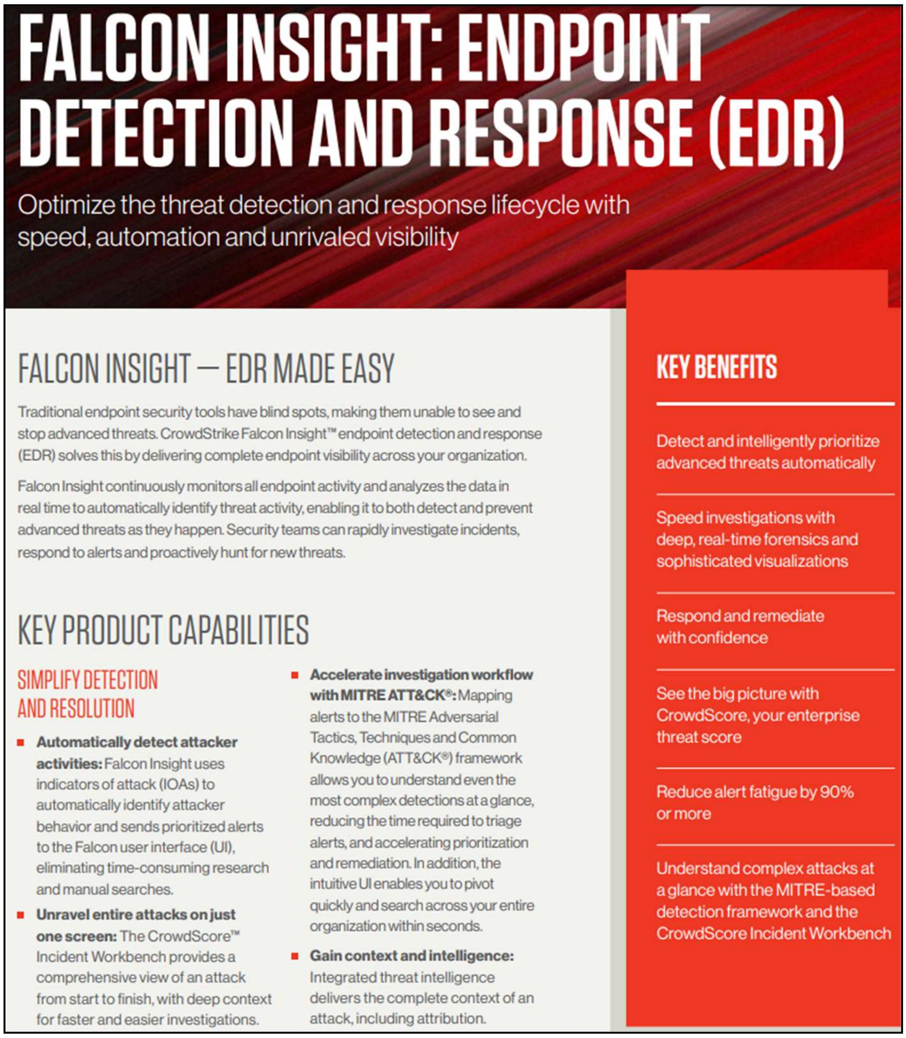
143. Paragraphs 1 through 35 are incorporated by reference as if fully set forth herein.

[80] https://www.crowdstrike.com/products/crowdstrike-support/
[81] *Id.*
[82] https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/

144. Defendants are not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '517 Patent.

145. Defendants have and continue to directly infringe at least claim 13 of the '517 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '517 Patent. Such products incorporate the Indicators of Attack (IOA) and CrowdScore features and include at least CrowdStrike Falcon Insight EDR (with Falcon Agent) (the "'517 Accused Product") which is a system for assessing runtime risk for an application program that executes on a device, comprising: a rules database storing a plurality of rules, wherein each rule identifies an action sequence; a policy database storing a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules; and a runtime monitor including a processing device identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application, and identifying a behavior score for the application program that executes on the device based on the identified runtime risk, wherein the action sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action.

146. Every '517 Accused Product is a system for assessing runtime risk for an application program that executes on a device. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) assesses runtime risk for applications that execute on endpoints.



FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

KEY PRODUCT CAPABILITIES

SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

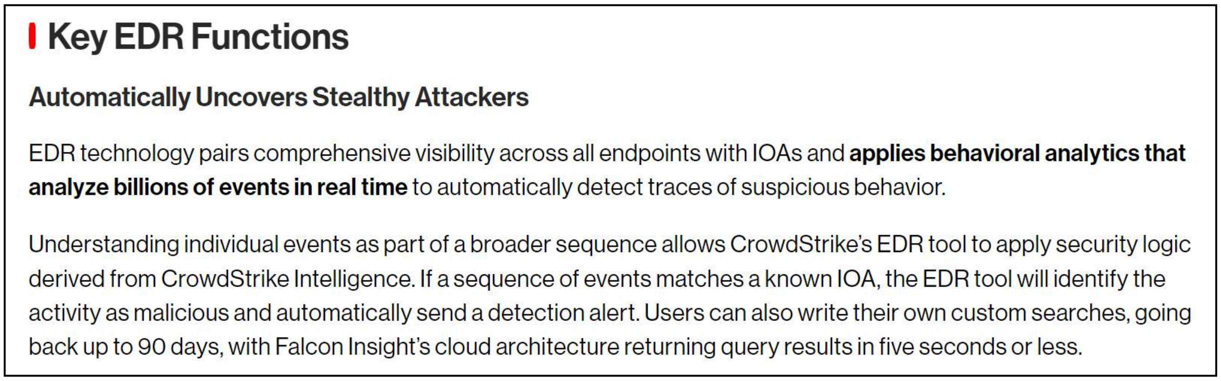
Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

[83]

147. Every ’517 Accused Product comprises a rules database storing a plurality of rules, wherein each rule identifies an action sequence. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) stores IOAs where each rule identifies an action sequence.[84]

[83] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

[84] *Id*.



Key EDR Functions

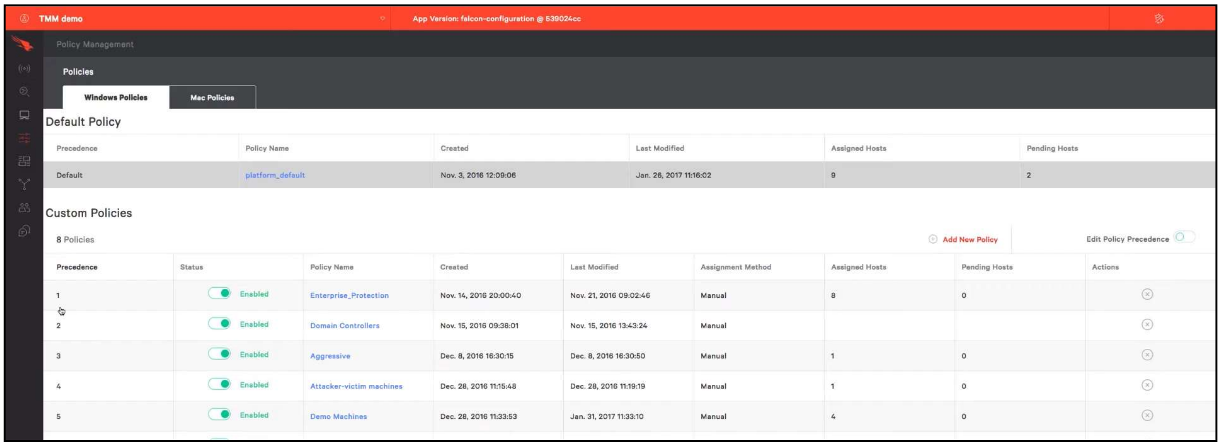
Automatically Uncovers Stealthy Attackers

EDR technology pairs comprehensive visibility across all endpoints with IOAs and **applies behavioral analytics that analyze billions of events in real time** to automatically detect traces of suspicious behavior.

Understanding individual events as part of a broader sequence allows CrowdStrike's EDR tool to apply security logic derived from CrowdStrike Intelligence. If a sequence of events matches a known IOA, the EDR tool will identify the activity as malicious and automatically send a detection alert. Users can also write their own custom searches, going back up to 90 days, with Falcon Insight's cloud architecture returning query results in five seconds or less.

[85]

148. Every '517 Accused Product comprises a policy database storing a plurality of assessment policies, wherein each assessment policy includes at least one rule of the plurality of rules. For example, at least CrowdStrike Falcon Insight EDR (with Falcon Agent) stores a plurality of assessment polices which comprise at least one rule of the plurality or rules.



Default Policy

Precedence	Policy Name	Created	Last Modified	Assigned Hosts	Pending Hosts
Default	platform_default	Nov. 3, 2016 12:09:06	Jan. 26, 2017 11:16:02	9	2

Custom Policies

8 Policies

Precedence	Status	Policy Name	Created	Last Modified	Assignment Method	Assigned Hosts	Pending Hosts	Actions
1	Enabled	Enterprise_Protection	Nov. 14, 2016 20:00:40	Nov. 21, 2016 09:02:46	Manual	8	0	⊗
2	Enabled	Domain Controllers	Nov. 15, 2016 09:38:01	Nov. 15, 2016 13:43:24	Manual			⊗
3	Enabled	Aggressive	Dec. 8, 2016 16:30:15	Dec. 8, 2016 16:30:50	Manual	1	0	⊗
4	Enabled	Attacker-victim machines	Dec. 28, 2016 11:15:48	Dec. 28, 2016 11:19:19	Manual	1	0	⊗
5	Enabled	Demo Machines	Dec. 28, 2016 11:33:53	Jan. 31, 2017 11:33:10	Manual	4	0	⊗

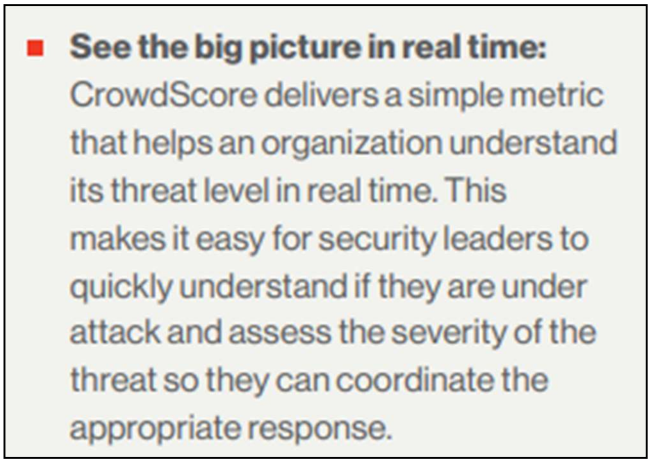
[86]

149. Every '517 Accused Product comprises a runtime monitor including a processing device identifying, using at least one assessment policy, a runtime risk for an application program that executes on a device, wherein the identified runtime risk indicates a risk or threat of the identified action sequence of the application, and identifying a behavior score for the application program that executes on the device based on the identified runtime risk, wherein the action

[85] https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

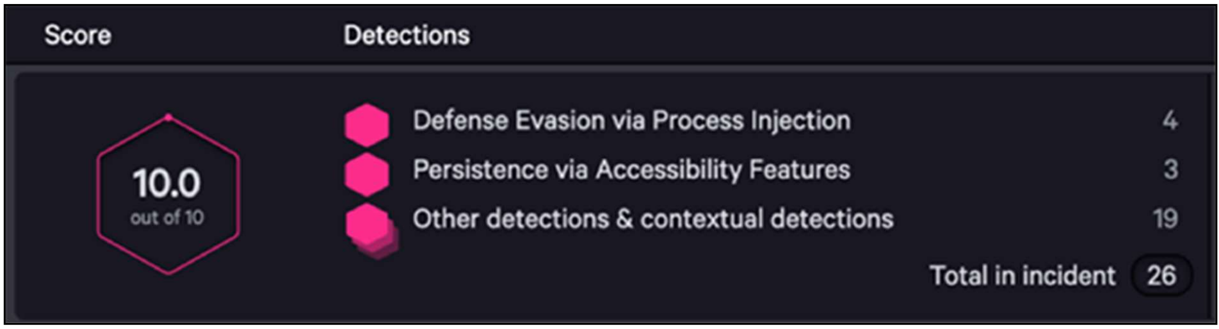
[86] https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/

sequence is a sequence of at least two performed actions, and each performed action is at least one of: a user action, an application action, and a system action. For example, CrowdStrike Falcon Insight EDR (with Falcon Agent) comprises a runtime monitor which uses assessment policies to identify a runtime risk for an application program that executes on an endpoint. The identified runtime risk indicates a risk or threat of the identified action sequence of the application (*e.g.*, IOA). CrowdStrike Falcon Insight EDR (with Falcon Agent) identifies a CrowdScore for the application program based on the identified runtime risk. The action sequence is a sequence of at least two performed actions and each action is at least one of a user action, an application action, and a system action.



- **See the big picture in real time:** CrowdScore delivers a simple metric that helps an organization understand its threat level in real time. This makes it easy for security leaders to quickly understand if they are under attack and assess the severity of the threat so they can coordinate the appropriate response.

[87]



Score	Detections	
10.0 out of 10	Defense Evasion via Process Injection	4
	Persistence via Accessibility Features	3
	Other detections & contextual detections	19
	Total in incident	26

[88]

[87] https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf

[88] https://www.crowdstrike.com/press-releases/crowdstrike-introduces-crowdscore/

150. Defendants have and continue to indirectly infringe one or more claims of the ’517 Patent by knowingly and intentionally inducing others, including CrowdStrike subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as the ’517 Accused Product (*e.g.*, products that incorporate the Correlated Rule and/or Targeted Attack Campaign features).

151. Defendants with knowledge that these products, or the use thereof, infringe the ’517 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continue to knowingly and intentionally induce, direct infringement of the ’517 Patent by providing these products to end-users for use in an infringing manner, as well as providing instruction and installation manuals on their support portal, and providing customer service through phone support and/or dedicated support staff that instruct end-users to use the products in an infringing manner.[89]

152. Defendants encourage and induce their customers of the Accused Products to perform the methods claimed in the Asserted Patents. For example, CrowdStrike makes its security services available on its website, widely advertises those services, provides applications that allow partners and users to access those services, provides instructions for installing and maintaining those products, and provides technical support to users via the CrowdStrike support portal.[90]

153. CrowdStrike further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging the “CrowdStrike Falcon agent” to be installed on individual endpoint computers.[91]

[89] https://www.crowdstrike.com/products/crowdstrike-support/

[90] *Id.*

[91] https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/

154. Defendants have induced and are currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’517 Patent, but while remaining willfully blind to the infringement.

155. Taasera Licensing has suffered damages as a result of Defendants’ direct and indirect infringement of the ’517 Patent in an amount to be proved at trial.

156. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendants’ infringement of the ’517 Patent, for which there is no adequate remedy at law, unless Defendants’ infringement is enjoined by this Court.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Taasera Licensing prays for relief against Defendants as follows:

a. Entry of judgment declaring that Defendants have directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;

b. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendants, their officers, agents, servants, employees, attorneys, and those persons in active concert or participation with the, from further acts of infringement of the Patents-in-Suit;

c. An order awarding damages sufficient to compensate Taasera Licensing for Defendants’ infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;

d. Entry of judgment declaring that this case is exceptional and awarding Taasera Licensing its costs and reasonable attorney fees under 35 U.S.C. § 285; and,

e. Such other and further relief as the Court deems just and proper.

Dated: October 21, 2022

Respectfully submitted,

/s/ *Raymond W. Mort, III*
Raymond W. Mort, III
Texas Bar No. 00791308
Email: raymort@austinlaw.com
THE MORT LAW FIRM, PLLC
501 Congress Avenue, Suite 150
Austin, Texas 78701
Tel/Fax: 512-865-7950

OF COUNSEL:

/s/ *Alfred R. Fabricant*
Alfred R. Fabricant (*pro hac vice* to be filed)
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos (*pro hac vice* to be filed)
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III (*pro hac vice* to be filed)
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
Joseph M. Mercadante (*pro hac vice* to be filed)
NY Bar No. 4784930
Email: jmercadante@fabricantllp.com
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

ATTORNEYS FOR PLAINTIFF
TAASERA LICENSING LLC